administration guide

hp StorageWorks NAS 1000s

First Edition (April 2003)

Part Number: 338724-001

This guide provides information on performing the administrative tasks necessary to manage the HP StorageWorks NAS 1000s server. Overview information as well as procedural instructions are included in this guide.

© Copyright 2003 Hewlett-Packard Development Company, L.P.

Hewlett-Packard Company makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard. The information contained in this document is subject to change without notice.

Compaq Computer Corporation is a wholly-owned subsidiary of Hewlett-Packard Company.

Microsoft®, MS-DOS®, Windows®, and Windows NT® are trademarks of Microsoft Corporation in the U.S. and/or other countries.

Intel and Pentium are trademarks of Intel Corporation in the U.S. and/or other countries.

UNIX® is a trademark of The Open Group in the U.S. and/or other countries.

All other product names mentioned herein may be trademarks of their respective companies.

Hewlett-Packard Company shall not be liable for technical or editorial errors or omissions contained herein. The information is provided "as is" without warranty of any kind and is subject to change without notice. The warranties for Hewlett-Packard Company products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty.

NAS 1000s Administration Guide
First Edition (April 2003)
Part Number: 338724-001

contents

About this Guide 11
Overview 12
Intended Audience 12
Prerequisites 12
Conventions 13
Document Conventions 13
Text Symbols 13
Equipment Symbols 13
Rack Stability 15
Getting Help 15
HP Technical Support 15
HP Storage Website 16
HP Authorized Reseller 16

1 System Overview 17
Product Definition and Information 18
Server Hardware Features 18
Optional Features 19
Software Features 19
Product Information 19
Product Manageability 20
Product Redundancy 20
Product Scalability 20
Deployment Scenarios 21
Environment Scenarios 22
Workgroup 22
Domain 22
User Interfaces 23
NAS 1000s Web-Based User Interface 23
Status 23
Network 24
Disks 24
Users 24
Shares 24
Maintenance 24
HP Utilities 24
Help 24

Take a Tour 24
Rapid Startup Wizard 24
Set Server Appliance Name 24
Set Administrator Password 24
Set Default Page 24
NAS 1000s Desktop 25
NAS Management Console 26
Install Data Copy 26

2 Setup Completion and Basic Administrative Procedures 27
Setup Completion 28
Managing System Storage 28
Creating and Managing Users and Groups 28
Creating and Managing File Shares 29
Installing and Configuring Data Replication Software 30
Basic Administrative Procedures 32
Setting the System Date and Time 33
Shutting Down or Restarting the Server 34
Viewing and Maintaining Audit Logs 35
Using Terminal Services 36
Setting up E-mail Alerts 36
Updating the Software 37
Changing System Network Settings 37

3 Persistent Storage Manager 39
Operational Overview 39
Reading Snapshots 40
Creating Snapshots 40
PSM Snapshot Attributes 40
Read Only 40
Read/Write 40
Always Keep 41
Automated Snapshot Deletion 41
Data Recovery 41
File/Folder/Volume Recovery 41
Snapshots and Drive Defragmentation 41
PSM and Backup 42
Snapshots Performance Impact 43
Recovering Snapshots after a System Restore or System Loss 43
Granule Size Update Utility 44
Clearing the Cache File from the System 45
Re-extending Volumes from Old Snapshots 45
Volume Display in Persistent Storage Manager 45
Persistent Storage Manager Storage Limitations 46
Accessing Persistent Storage Manager 46
Global Settings 47
Maximum Persistent Images 47
Inactive Period 47
Inactive time-out 48
Image directory 48

Restore Defaults 48
Volume Settings 48
Available Volume 48
Size 49
Free Space 49
Cache Size 49
Usage 49
Volume Configuration Settings 49
Warning threshold reached when 50
Begin deleting images when 50
Cache size 50
Schedules 50
Create a New Schedule 51
Editing Persistent Image Schedule Properties 52
Deleting a Persistent Image Schedule 53
Persistent Image and Group Information 54
Image name and location on volume 54
Persistent image group name 54
Number of images in group 54
Volumes included in this image 54
Image attributes 54
Retention weight 55
Most recent image in group 55
Oldest image in group 55
Next image in group to be deleted 55
Managing Persistent Images 55
Creating a New Persistent Image 56
Deleting a Persistent Image 57
Editing Persistent Image Properties 58
Undo Persistent Image Changes 59
Restoring an Image 60
Known Issues 62
Event log error at cache full 62
Display Error on SAK 62
Always Keep error at cache file full 62
Improper display of default Cache File Size 62
Page file setting 62
No Boot - No Revert 62
Reverting of System Drive Prohibited 62
No support for mount points in UNIX, AppleTalk, or NetWare 62

4 User and Group Management 63
Domain Compared to Workgroup Environments 64
User and Group Name Planning 64
Managing User Names 65
Managing Group Names 65
Workgroup User and Group Management 66
Managing Local Users 66
Adding a New User 67
Deleting a User 67

Modifying a User Password 68
Modifying User Properties 68
Managing Local Groups 69
Adding a New Group 70
Deleting a Group 70
Modifying Group Properties 71
General Tab 71
Members Tab 71
Drive Quotas 72
Managing Quotas 72
Enabling and Disabling Quota Management 74
Creating New Quota Entries for a User or Group 75
Deleting Quota Entries for a User or Group 76
Modifying Quota Entries for a User or Group 76

5 Folder and Share Management 79
Folder Management 80
Navigating to a Specific Volume or Folder 81
Creating a New Folder 82
Deleting a Folder 83
Modifying Folder Properties 83
Creating a New Share for a Volume or Folder 84
Managing Shares for a Volume or Folder 85
Managing File Level Permissions 86
Share Management 92
Share Considerations 92
Defining Access Control Lists 92
Integrating Local File System Security into Windows Domain Environments 93
Comparing Administrative (Hidden) and Standard Shares 93
Planning for Compatibility between File Sharing Protocols 93
NFS Compatibility Issues 93
Managing Shares 94
Creating a New Share 94
Deleting a Share 95
Modifying Share Properties 96
CIFS Sharing 96
NFS Sharing 98
FTP Sharing 98
Web Sharing (HTTP) 98
NetWare Sharing (NCP) 99
AFP (AppleTalk) Sharing 100
Installing Services for AppleTalk 100
Installing Windows NT Services for Macintosh 100
Protocol Parameter Settings 101
CIFS Protocol Settings 102
NFS Protocol Settings 102
FTP Protocol Settings 102
HTTP Protocol Settings 102
NCP (NetWare) Protocol Settings 102
AFP (AppleTalk) Protocol Settings 103

6 UNIX File System Management 105
Network File System 106
Server for NFS 106
Authenticating User Access 107
Indicating the Computer to Use for the NFS User Mapping Server 107
Logging Events 108
Installing NFS Authentication Software on the Domain Controllers and Active Directory Domain Controllers 109
NFS File Shares 110
Creating a New Share. 110
Deleting a Share. 111
Modifying Share Properties. 111
Encoding Types. 113
NFS Protocol Properties Settings 114
NFS Async/Sync Settings 115
NFS Locks 115
NFS Client Groups 117
Adding a New Client Group 118
Deleting a Client Group 118
Editing Client Group Information 119
NFS User and Group Mappings 120
Types of Mappings. 120
Explicit Mappings 120
Simple Mappings. 120
Squashed Mappings. 121
User Name Mapping Best Practices. 121
Creating and Managing User and Group Mappings 122
General Information 122
Simple Mapping 123
Explicit User Mapping. 124
Explicit Group Mapping 125
Backing up and Restoring Mappings 126
Backing up User Mappings 127
Restoring User Mappings 127
NFS File Sharing Tests. 128
Terminal Services, Telnet Service, and Remote Shell Service 129
Using Terminal Services 129
Using Telnet Server 129
Using Remote Shell Service. 129
Password Synchronization 130
Password Synchronization Best Practices 130
Password Synchronization Requirements 131
Implementing Password Synchronization 131
Configuring Advanced Settings 131
Installing Password Synchronization on Domain Controllers and Active Directory Domain Controllers 132
Customizing Password Synchronization 133

7 NetWare File System Management 135
Installing Services for NetWare 136
Managing File and Print Services for NetWare 137

Creating and Managing NetWare Users 138
Adding Local NetWare Users 138
Enabling Local NetWare User Accounts 139
Managing NCP Volumes (Shares) 140
Creating and Managing NCP File Shares Using the WebUI 140
Creating a New NCP Share 140
Deleting an NCP Share 141
Modifying NCP Share Properties 142
Creating and Managing NCP Shares using the NAS Management Console 143
Creating a New NCP Share using the NAS Management Console 144
Modifying NCP Share Properties using the NAS Management Console 147
NOTES:. 148

8 Remote Access Methods and Monitoring 149
Web Based User Interface 150
Terminal Services 150
Telnet Server. 151
Enabling Telnet Server. 151
Configuring Telnet Server 151
Authentication Information 151
Auditing Information 152
Server Settings 152
Sessions Information 152
Remote Shell Daemon 152

A Backup Management 153
Backup Solutions 153
System Environments. 153
SCSI Direct Connect Environments 153
Hardware Options 154
Software Options 154
Best Practices 155
Regular and Reliable Backups 155
Automated Tape Libraries 155
Multiple Backup Devices. 155
Backup Schedules 156
Media Rotation. 156
Offsite Storage 156
Server Setup Information Archival 156
Snapshots and Quick Online Restores 157
Readiness Testing. 158
Disaster Recovery 158

B PSM Error Codes 159

Index 167

Figures

1 Primary WebUI screen 23
2 NAS 1000s desktop 25

3 NAS data copy install wizard. . . . 31
4 Maintenance menu 32
5 Date and Time dialog box 33
6 Shutdown menu 34
7 Logs menu 35
8 Terminal Services session 36
9 Network menu 37
10 PSM Main screen 46
11 Global settings 47
12 Volume settings 48
13 Volume configuration settings 49
14 Persistent Image Schedules 50
15 Create Persistent Image Schedule 51
16 Edit schedule properties 52
17 Delete scheduled images 53
18 Persistent Image and Group Information 54
19 Managing persistent images 55
20 Create new persistent image. . . . 56
21 Delete Verification 57
22 Edit Persistent Image Properties 58
23 Undo Image Changes 59
24 Images available to restore 60
25 Restore confirmation screen. . . . 61
26 Local Users dialog box. . . . 66
27 Create New User dialog box 67
28 User Properties dialog box 68
29 Local Groups dialog box 69
30 Create New Group dialog box, General tab 70
31 Group Properties dialog box, General tab 71
32 Group Properties dialog box, Members tab 72
33 Disk Quota dialog box 73
34 Default Quota dialog box 74
35 Quota Entries dialog box 75
36 New Quota Entry dialog box 76
37 Quota Entry dialog box for a user 77
38 Volumes dialog box 81
39 Folders dialog box 82
40 Create a New Folder dialog box, General tab 83
41 Folder Properties dialog box, General tab 84
42 Create New Share dialog box, General tab 85
43 Security Properties dialog box for folder name NTSF Test. . . . 87
44 Access Control Settings dialog box for folder name NTSF Test, Permissions tab 88
45 User or Group Permission Entry dialog box for folder name NTSF Test 88
46 Access Control Settings, Auditing tab dialog box for folder name NTSF Test. . . . 89
47 Select User, Computer, or Group dialog box 90
48 Auditing Entry dialog box for folder name NTSF Test 90
49 Access Control Settings, Owner tab dialog box for folder name NTSF Test 91
50 Create a New Share dialog box, General tab 95
51 Share Properties dialog box, General tab 96
52 Share Properties dialog box, CIFS Sharing tab 97

53 Share Properties dialog box, NFS Sharing tab 98
54 Share Properties dialog box, NetWare Sharing tab 99
55 Local Area Connection Properties page, Install option 100
56 Sharing Protocols dialog box 101
57 NAS Management Console Server for NFS screen, User Mapping tab 108
58 NAS Management Console Server for NFS screen, Logging tab 108
59 Create a New Share dialog box, General tab 110
60 Share Properties dialog box, General tab 112
61 NFS Sharing tab 112
62 NFS Sharing Protocols menu 114
63 NFS Async/Sync Settings dialog box 115
64 NFS Locks dialog box 116
65 NFS Client Groups dialog box 117
66 New NFS Client Group dialog box 118
67 Client Groups dialog box 119
68 Edit NFS Client Groups dialog box 119
69 Mapping Server "ls -al" Command example 121
70 User and Group Mappings dialog box, General tab 123
71 User and Group Mappings dialog box, Simple Mapping tab 124
72 User and Group Mappings dialog box, Explicit User Mapping tab 125
73 User and Group Mappings dialog box, Explicit Group Mapping tab 126
74 NAS Management Console User Name Mapping screen, Map Maintenance tab 127
75 Password Synchronization screen 130
76 Password Synchronization screen, Advanced Settings dialog box 132
77 Local Area Connection Properties page, Install option 136
78 Installing File and Print Services for NetWare 137
79 File and Print Services for NetWare screen 137
80 New User dialog box 138
81 NetWare Services tab 139
82 Create a New Share dialog box, General tab 141
83 Share Properties dialog box, General tab 142
84 Share Properties dialog box, NetWare Sharing tab 143
85 Create Shared Folder dialog box 144
86 NetWare Basic Share Permissions dialog box 145
87 Customize Permissions dialog box, Share Permissions tab 146
88 Customize Permissions dialog box, Security tab 147
89 Telnet Server interface screen 151

Tables

1 Document Conventions 13
2 Adjusting Granule Size 44
3 Group Name Examples 65
4 Command Line Interface Command Prompts 129
5 PSM Error Codes 159

about this guide

This administration guide provides information to help you:

- Plan your storage configuration
- Set up physical storage
- Set up virtual storage
- Manage users and groups
- Manage folders and shares
- Manage a UNIX® file system
- Manage a NetWare file system
- Remotely access the HP StorageWorks NAS 1000s server

About this Guide topics include:

- Overview, page 12
- Conventions, page 13
- Rack Stability, page 15
- Getting Help, page 15

Overview

This section covers the following topics:

- Intended Audience
- Prerequisites
- Conventions

Intended Audience

This book is intended for use by system administrators who are experienced with setting up and managing a network server.

Prerequisites

Before beginning, make sure you consider the following:

- Knowledge of Microsoft® Windows NT or 2000 operating systems
- Knowledge of HP hardware
- Location of all documentation shipped with your device

Conventions

Conventions consist of the following:

- Document Conventions
- Text Symbols
- Equipment Symbols

Document Conventions

The document conventions included in Table 1 apply in most cases.

Table 1: Document Conventions

Element	Convention
Cross-reference links	Figure 1
Key and field names, menu items, buttons, and dialog box titles	**Bold**
File names, application names, and text emphasis	Italics
User input, command and directory names, and system responses (output and messages)	`Monospace font` `COMMAND NAMES` are uppercase monospace font unless they are case sensitive
Variables	*`<monospace, italic font>`*
Website addresses	Underlined sans serif font text: http://www.hp.com

Text Symbols

The following symbols may be found in the text of this guide. They have the following meanings.

WARNING: Text set off in this manner indicates that failure to follow directions in the warning could result in bodily harm or death.

Caution: Text set off in this manner indicates that failure to follow directions could result in damage to equipment or data.

Note: Text set off in this manner presents commentary, sidelights, or interesting points of information.

Equipment Symbols

The following equipment symbols may be found on hardware for which this guide pertains. They have the following meanings.

Any enclosed surface or area of the equipment marked with these symbols indicates the presence of electrical shock hazards. Enclosed area contains no operator serviceable parts.

WARNING: To reduce the risk of personal injury from electrical shock hazards, do not open this enclosure.

Any RJ-45 receptacle marked with these symbols indicates a network interface connection.

WARNING: To reduce the risk of electrical shock, fire, or damage to the equipment, do not plug telephone or telecommunications connectors into this receptacle.

Any surface or area of the equipment marked with these symbols indicates the presence of a hot surface or hot component. Contact with this surface could result in injury.

WARNING: To reduce the risk of personal injury from a hot component, allow the surface to cool before touching.

Power supplies or systems marked with these symbols indicate the presence of multiple sources of power.

WARNING: To reduce the risk of personal injury from electrical shock, remove all power cords to completely disconnect power from the power supplies and systems.

Any product or assembly marked with these symbols indicates that the component exceeds the recommended weight for one individual to handle safely.

WARNING: To reduce the risk of personal injury or damage to the equipment, observe local occupational health and safety requirements and guidelines for manually handling material.

Rack Stability

Rack stability protects personal and equipment.

WARNING: To reduce the risk of personal injury or damage to the equipment, be sure that:

- The leveling jacks are extended to the floor.
- The full weight of the rack rests on the leveling jacks.
- In single rack installations, the stabilizing feet are attached to the rack.
- In multiple rack installations, the racks are coupled.
- Only one rack component is extended at any time. A rack may become unstable if more than one rack component is extended for any reason.

Getting Help

If you still have a question after reading this guide, contact an HP authorized service provider or access our website: http://www.hp.com.

HP Technical Support

In North America, call technical support at 1-800-652-6672, available 24 hours a day, 7 days a week.

Note: For continuous quality improvement, calls may be recorded or monitored.

Outside North America, call technical support at the nearest location. Telephone numbers for worldwide technical support are listed on the HP website under support: http://www.hp.com..

Be sure to have the following information available before calling:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages
- Operating system type and revision level
- Detailed, specific questions

HP Storage Website

The HP website has the latest information on this product, as well as the latest drivers. Access storage at: http://www.hp.com.. From this website, select the appropriate product or solution.

HP Authorized Reseller

For the name of your nearest HP authorized reseller:

- In the United States, call 1-800-345-1518
- In Canada, call 1-800-263-5868
- Elsewhere, see the HP website for locations and telephone numbers: http://www.hp.com.

System Overview

1

The HP StorageWorks NAS 1000s server can be used in many types of computing environments, from basic Microsoft Windows workgroups to complicated multiprotocol domains using CIFS, NFS, NCP, AppleTalk, FTP, and HTTP. The corresponding varieties of clients that can be serviced include any Windows, UNIX, Linux, Novell, or Macintosh variant.

This chapter provides an overview of these environments and deployments and includes brief descriptions of system user interfaces, applications, and options.

- Product Definition and Information
  - Server Hardware Features
  - Software Features
  - Product Information
- Deployment Scenarios
- Environment Scenarios
- User Interfaces
  - NAS 1000s Web Based User Interface
  - NAS 1000s Console

Note: The NAS 1000s Console can be accessed via a directly connected keyboard and mouse, or using Terminal Services.

Product Definition and Information

The NAS 1000s is a business class NAS solution that provides reliable performance, manageability, and fault tolerance.

Server Hardware Features

The following features are included in the NAS 1000s Model 1 server:

- Intel Pentium 4 2.4 GHz processor
- 512-MB 200 MHz PC2100 DDR SDRAM memory
- 64-bit PCI-X slot
- 64-bit PCI slot
- Four 80GB 7200 rpm hot-pluggable hard drives
- Two embedded 10/100/1000 WOL (Wake on LAN) network interface controllers (NICs)
- SCSI Controller for tape backup

The following features are included in the NAS 1000s Model 2 server:

- Intel Pentium 4 2.8 GHz processor
- 512-MB 200 MHz PC2100 DDR SDRAM memory
- 64-bit PCI-X slot
- 64-bit PCI slot
- Four 160GB 7200 rpm hot-pluggable hard drives
- Two embedded 10/100/1000 WOL (Wake on LAN) network interface controllers (NICs)
- SCSI Controller for tape backup

The following features are included in the NAS 1000s Model 3 server:

- Intel Pentium 4 2.8 GHz processor
- 512-MB 200 MHz PC2100 DDR SDRAM memory
- 64-bit PCI-X slot
- 64-bit PCI slot
- Four 250GB 7200 rpm hot-pluggable hard drives
- Two embedded 10/100/1000 WOL (Wake on LAN) network interface controllers (NICs)
- SCSI Controller for tape backup

Optional Features

The following features are optional for the NAS 1000s server:

- Additional memory
- Network interface cards (NICs)
- Tape drive
- SAN Fibre Channel Adapter for tape backup

Software Features

Advanced features included and supported by the NAS 1000s include:

- Microsoft Services for Macintosh
- Microsoft Services for NetWare
- Microsoft Services for UNIX (SFU)
- NAS Web Based User Interface (WebUI)
- StorageWorks Data Copy (Trial Version)
- Windows Powered OS
- Columbia Data Products Persistent Storage Manager
- Optional third party supported software (not included):
  - Backup software
  - Management software
  - Quota management
  - Virus protection

For specific software product recommendations, go to the HP website:

http://h18000.www1.hp.com/products/storageworks/nas/supportedsoftware.html

Product Information

The NAS 1000s provides performance gains over general purpose servers by integrating optimized hardware components and specialized software. Integrating NAS devices into the network improves the performance of existing servers because NAS devices are optimized for file serving tasks.

Product Manageability

The NAS 1000s ships with the following utilities and features that ease the administration tasks associated with managing the system:

- The Rapid Startup Utility is a user friendly configuration utility that ensures easy configuration.
- The WebUI is a simple, graphical user interface (GUI) that helps with administration tasks.

Product Redundancy

The NAS 1000s is specifically designed to perform file serving tasks for networks, using industry standard components to ensure reliability.

Other industry standard features, such as redundant array of independent drives (RAID) and remote manageability, further enhance the overall dependability of the NAS 1000s.

To ensure redundancy and reliability, the hard drives installed in the NAS 1000s are configured so that a single drive failure will not cause data loss or system failure. The NAS 1000s is configured a with dual boot capibility. When powered on, the NAS 1000s can boot using a primary OS or a secondary recovery OS. The primary OS resides on drive 0 and is mirrored on drive 1 while the secondary OS resides on drive 2 and is mirrored on drive 3. If the primary OS becomes corrupted and un-bootable, the secondary OS is available for data backup prior to using the Quick Restore DVD to restore the system to the factory default state.

The data volume is configured as a RAID 5 volume across all four drives. This ensures redundancy in the event of a drive failure and the data volume is accessible by both the primary OS and secondary OS.

Product Scalability

The NAS 1000s offers optimized performance for a growing environment. Storage capacity can increase as a business grows without downtime or compromised performance. Internally the NAS 1000s can grow up to four data drives. With four 250GB disk drives storage capacity, it can grow up to 1TB of raw storage.

Deployment Scenarios

The default shipping configuration contains two 10/100/1000 integrated network interface controller (NIC) ports for client data access. These data ports also allow access to the Web user interface (WebUI) that accompanies the product. It is from the WebUI that most management and administrative procedures can be accomplished.

Typical deployment scenarios include:

- **File server consolidation**

  As businesses continue to expand their information technology (IT) infrastructures, they must find ways to manage larger environments without a corresponding increase in IT staff. Consolidating many servers into a single NAS device decreases the number of points of administration and increases the availability and flexibility of storage space.

- **Multiprotocol environments**

  Some businesses require several types of computing systems to accomplish various tasks. The multiprotocol support of the NAS 1000s allows it to support many types of client computers concurrently.

- **Protocol and platform transitions**

  When a transition between platforms is being planned, the ability of the NAS 1000s to support most file sharing protocols allows companies to continue to invest in file storage space without concerns about obsolescence. For example, an administrator planning a future transition from Windows to Linux can deploy the NAS 1000s with confidence that it can support both CIFS and NFS simultaneously, assuring not only a smooth transition, but also a firm protection of their investment.

- **Remote office deployment**

  Frequently, branch offices and other remote locations lack dedicated IT staff members. An administrator located in a central location can use the WebUI of the NAS 1000s, and Microsoft Terminal Services to configure and administer all aspects of the NAS 1000s.

Environment Scenarios

The NAS 1000s is deployed into one of two modes:

- Workgroup
- Domain (Windows NT Domain or Active Directory Domain)

The NAS 1000s uses standard Windows user and group administration methods in each of these environments. For procedural instructions on managing users and groups, see Chapter 4, User and Group Management, of this guide.

Regardless of the deployment, the NAS 1000s integrates easily into multiprotocol environments, supporting a wide variety of clients. The following protocols are supported:

- Common Internet File System (CIFS)
- Network File System (NFS)
- NetWare Core Protocol (NCP)
- Hypertext Transfer Protocol (HTTP)
- File Transfer Protocol (FTP)
- AppleTalk for Macintosh (AFP, also called MAC)

Workgroup

In a workgroup environment, users and groups are stored and managed separately, on each member server of the workgroup. Workgroups are typical for very small deployments where little or no computing environment planning is required.

Domain

When operating in a Windows NT or Active Directory domain environment, the NAS 1000s is a member of the domain and the domain controller is the repository of all account information. Client machines are also members of the domain and users log on to the domain through their Windows based client machines. The domain controller also administers user accounts and appropriate access levels to resources that are a part of the domain. Additional information about planning for domain environments can be found at:

http://www.microsoft.com/windows2000/technologies/directory/ad/default.asp

The NAS 1000s obtains user account information from the domain controller when deployed in a domain environment. The NAS 1000s itself cannot act as a domain controller.

User Interfaces

There are several user interfaces that administrators can use to access and manage the NAS 1000s. Two of these interfaces are:

- NAS 1000s WebUI
- NAS 1000s Console

Each interface contains the same or similar capabilities, but presents them in a different manner. Each of these interfaces are illustrated in the following sections.

NAS 1000s Web-Based User Interface

The WebUI provides for system administration, including user and group management, share management, and local storage management.

To access the WebUI, launch a Web browser and enter the following in the address field:

```
http://<your NAS machine name or IP Address>:3201/
```

Extensive online help for the WebUI is available by clicking **Help** on the primary WebUI screen.

The primary screen of the WebUI is shown in Figure 1.

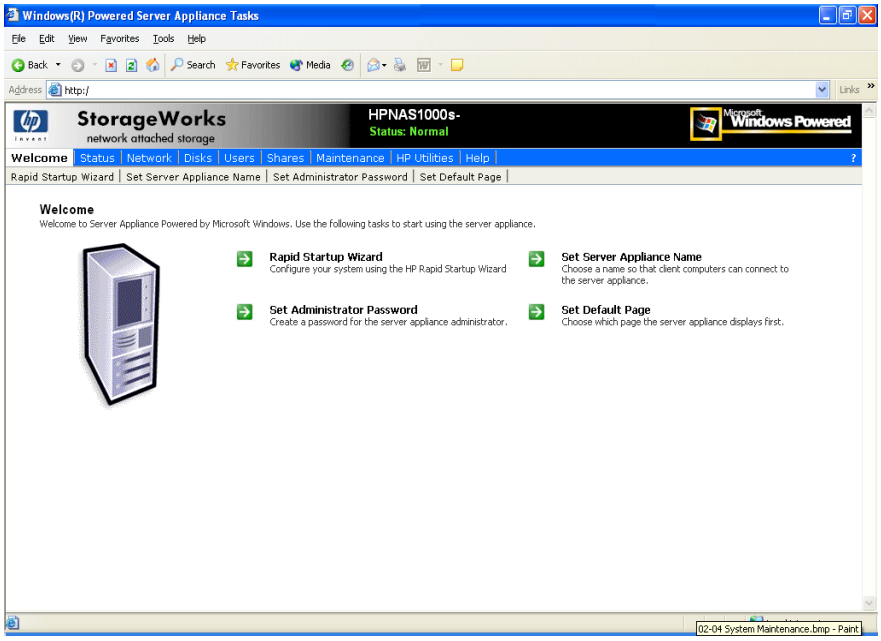
Windows(R) Powered Server Appliance Tasks
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http:/
Links
StorageWorks
network attached storage
HPNAS1000s-
Status: Normal
Microsoft Windows Powered
Welcome Status Network Disks Users Shares Maintenance HP Utilities Help
Rapid Startup Wizard Set Server Appliance Name Set Administrator Password Set Default Page
Welcome
Welcome to Server Appliance Powered by Microsoft Windows. Use the following tasks to start using the server appliance.
Rapid Startup Wizard
Configure your system using the HP Rapid Startup Wizard
Set Server Appliance Name
Choose a name so that client computers can connect to the server appliance.
Set Administrator Password
Create a password for the server appliance administrator.
Set Default Page
Choose which page the server appliance displays first.
02-04 System Maintenance.bmp - Paint

Figure 1: Primary WebUI screen

As shown in Figure 1, the following areas are administered through this interface:

Status

The Status option displays system information, including disk status data and system information.

Network

The Network option contains system settings, including system identification, global settings, interfaces settings, administration settings, Telnet settings, and SNMP settings.

Disks

Use this option to manage disks, volumes, and disk quotas, and snapshots.

Users

When deployed, the administrator uses this option to manage local users and groups. Local users and groups are discussed in Chapter 4, User and Group Management.

Shares

The administrator creates folders and shares to control access to files. When a share is created, the administrator indicates the protocols that can be supported by that share as well as the users and groups of users that have access. Protocol parameters are entered in this Shares option. See Chapter 5, Folder and Share Management, for additional information.

Maintenance

Maintenance tasks include setting date and time, performing system restarts and shutdowns, viewing audit logs, accessing Terminal Services, and setting up Email alerts.

HP Utilities

Access HP system management utilities such as NAS Data Copy.

Help

This option contains help information for the WebUI.

Take a Tour

Take a tour and learn how to use your server appliance.

Rapid Startup Wizard

Use this utility to enter system setup and configuration information.

Set Server Appliance Name

Choose a name so that client computers can connect to the server appliance.

Set Administrator Password

Create a password for the server appliance administrator.

Set Default Page

Choose which page the server appliance displays first.

NAS 1000s Console

The NAS 1000s Console can be accessed by:

- Directly connecting a keyboard and mouse
- Using the WebUI Maintenance tab and selecting **Terminal Services**

Note: When using Terminal Services to connect to the NAS 1000s Console do not use the window close feature ( ). Click on **Start/Log Off Administrator** to exit Terminal Services.

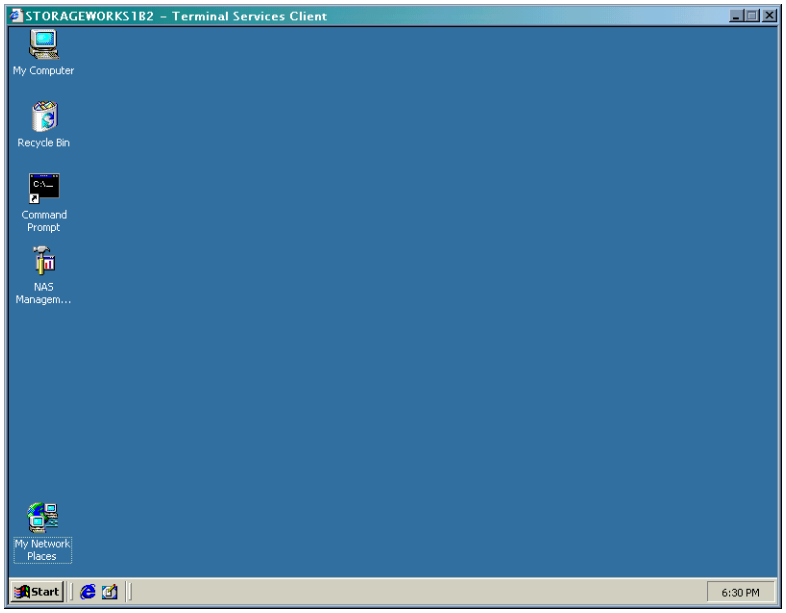

Figure 2: NAS 1000s Console

The following icons are available from the Desktop:

- NAS Management Console
- Install Data Copy

NAS Management Console

Click this icon to access the following folders:

- **Core Operating System** is used to manage local users and groups, access performance logs and alerts, and manage the event viewer.
- **Disk System** contains access to local disk management, including a volume list and a graphical view of the disks.
- **File Sharing** contains modules for the configuration of file sharing exports. CIFS (Windows) and NFS (UNIX) file shares are managed through this folder.
- **System** contains system summary information.

Data Copy

StorageWorks NAS Data Copy is a real time data replication and failover software product that augments existing data protection and tape backup strategies. This product is not intended to replace regular tape backups.

Download and install a free 30-day trial version of Data Copy from the software and driver link of the NAS 1000s product page. To access the NAS 1000s product page:

go to www.hp.com

1. select storage
2. select network attached storage from the networked storage options.
3. select the NAS 1000s
4. select software and drivers

See Chapter 2, Setup Completion and Basic Administrative Procedures, for additional information.

Setup Completion and Basic Administrative Procedures

2

This chapter continues the process of setting up the system that was started using the HP StorageWorks NAS 1000s Quick Start Guide by discussing additional setup procedures and options.

Basic system administration functions are also included in this chapter.

Unless otherwise instructed, all procedures are performed using the NAS Web Based User Interface (WebUI).

The following topics are included in this chapter:

- Setup completion
  - Managing system storage
  - Creating and managing users and groups
  - Creating and managing file shares
  - Installing and configuring data replication software
- Basic administrative procedures
  - Setting the system date and time
  - Powering down and restarting the server
  - Viewing and maintaining audit logs
  - Using terminal services
  - Setting up email alerts
  - Updating the software
  - Changing system network settings

Setup Completion

After the NAS device is physically set up and the basic configuration is established, additional setup steps must be completed. Depending on the deployment scenario of the NAS device, these steps may vary.

Additional setup steps may include:

- Managing system storage
- Creating and managing users and groups
- Creating and managing file shares
- Installing and configuring data replication software

Each of these setup steps is discussed in the following sections.

Managing System Storage

The NAS administrator uses Logical Disk Manager to manage disks and volumes, and uses Persistent Storage Manager to manage snapshots. See the following chapters for more detailed information on managing system storage:

- Chapter 3, Persistent Storage Manager, discusses snapshot management procedures.
- Chapter 5, Folder and Share Management, discusses folder and share management procedures.

Creating and Managing Users and Groups

User and group information and permissions determine whether a user can access files. If the NAS device is deployed into a workgroup environment, this user and group information is stored locally on the device. By contrast, if the NAS device is deployed into a domain environment, user and group information is stored on the domain.

To enter local user and group information, see Chapter 4, User and Group Management.

The following information is included:

- Domain compared to workgroup environments
- User and group name planning
  - Managing user names
  - Managing group names
- Workgroup user and group management
  - Managing local users
  - Managing local groups
- Drive quotas
  - Managing quotas
  - Enabling and disabling quota management
  - Creating new quota entries for a user or group
  - Deleting new quota entries for a user or group
  - Modifying new quota entries for a user or group

Creating and Managing File Shares

Files shares must be set up, granting and controlling file access to users and groups. See Chapter 5, Folder and Share Management for complete information on managing file shares.

The following information is included:

- Folder Management
  - Navigating to a specific volume or folder
  - Creating a new folder
  - Deleting a folder
  - Modifying folder properties
  - Creating a new share for a volume or folder
  - Managing shares for a volume or folder
  - Managing file level permissions
- Share Management
  - Share considerations
  - Defining Access Control Lists
  - Integrating local file system security into Windows domain environments
  - Comparing administrative (hidden) and standard shares
  - Planning for compatibility between file sharing protocols
  - Managing shares
- Protocol parameter settings

UNIX specific information is discussed in Chapter 6, UNIX File System Management.

Installing and Configuring Data Replication Software

Data replication is the process of making a copy of system data. StorageWorks NAS Data Copy is a real time data replication and failover software product that augments existing data protection and tape backup strategies. This product is not intended to replace regular tape backups.

Using NAS Data Copy, mission critical data and data that must be protected is marked. NAS Data Copy replicates this data in real time from the production machine (source) to a backup machine (target). The target machine can be either on site or off site. After the initial copy out, NAS Data Copy monitors any changes to the specified data files and sends only the changes to the target machine.

NAS Data Copy can operate in many different system environments, including:

- **Single machine**—Source and target components are loaded on the same machine, allowing data to be replicated from one location to another on the same machine.
- **One-to-one**—One target machine, having no production activity, is dedicated to support one source machine. An alternative one-to-one scenario is when each machine acts both as a source and a target, actively replicating data to each other.
- **Many-to-one**—Many source machines are protected by one target machine.
- **One-to-many**—One source machine sends data to multiple target machines. The target machines may or may not communicate with each other.
- **Chained**—One or more source machines send replicated data to a target machine that in turn acts as a source machine and sends selected data to a final target machine.

NAS Data Copy is supported for all deployments of the NAS 1000s.

To download and install a free 30-day trial version of Data Copy:

go to www.hp.com

1. select storage
2. select network attached storage from the networked storage options.
3. select the NAS 1000s
4. select software and drivers
5. Double-click on the downloaded file, then follow the onscreen instructions.

StorageWorks NAS Data Copy Setup
hp StorageWorks NAS data copy
powered by NSI Software's Double-Take
Welcome to the StorageWorks NAS Data Copy Setup wizard
Certified For
Microsoft Windows
Windows 2000 Datacenter Server
Windows 2000 Advanced Server
Windows 2000 Server
The InstallShield® Setup wizard will install StorageWorks NAS Data Copy version 4.2.1.0.1067.5 on your computer. To continue, click Next.
< Back
Next >
Cancel

Figure 3: NAS data copy install wizard

Basic Administrative Procedures

Basic administrative procedures include:

- Setting the system date and time
- Shutting down or restarting the server
- Viewing and maintaining audit logs
- Using Terminal Services
- Setting up email alerts
- Updating the software
- Changing system network settings

These functions are performed in the **Maintenance** menu of the WebUI.

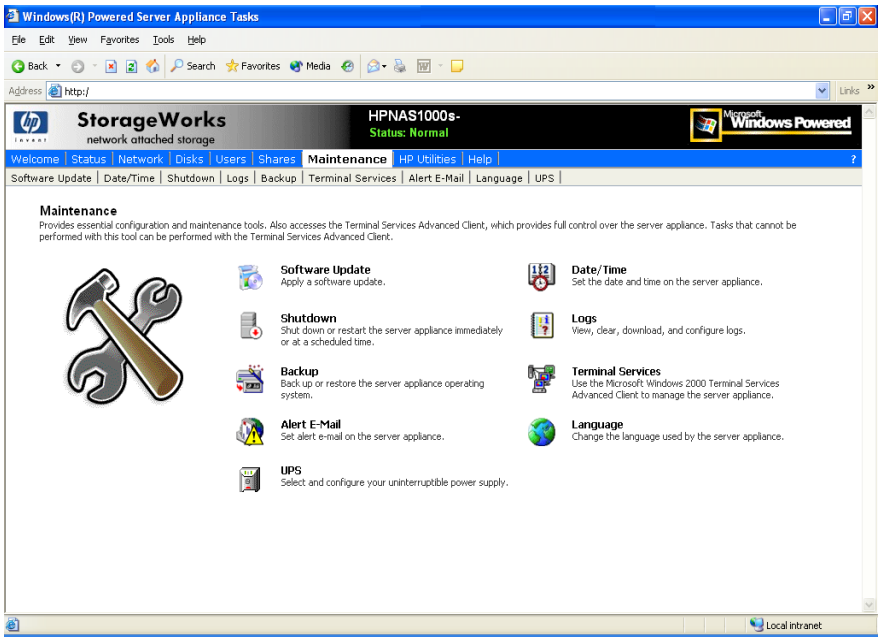
Windows(R) Powered Server Appliance Tasks
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http:/
Links
StorageWorks
network attached storage
HPNAS1000s-
Status: Normal
Microsoft Windows Powered
Welcome Status Network Disks Users Shares Maintenance HP Utilities Help
Software Update Date/Time Shutdown Logs Backup Terminal Services Alert E-Mail Language UPS
Maintenance
Provides essential configuration and maintenance tools. Also accesses the Terminal Services Advanced Client, which provides full control over the server appliance. Tasks that cannot be performed with this tool can be performed with the Terminal Services Advanced Client.
Software Update
Apply a software update.
Date/Time
Set the date and time on the server appliance.
Shutdown
Shut down or restart the server appliance immediately or at a scheduled time.
Logs
View, clear, download, and configure logs.
Backup
Back up or restore the server appliance operating system.
Terminal Services
Use the Microsoft Windows 2000 Terminal Services Advanced Client to manage the server appliance.
Alert E-Mail
Set alert e-mail on the server appliance.
Language
Change the language used by the server appliance.
UPS
Select and configure your uninterruptible power supply.
Local intranet

Figure 4: Maintenance menu

Setting the System Date and Time

To change the system date or time:

1. From the WebUI, select **Maintenance** and **Date/Time**. The **Date and Time Settings** dialog box is displayed.
2. Enter the new values and then click **OK**. The **Maintenance** menu is displayed.

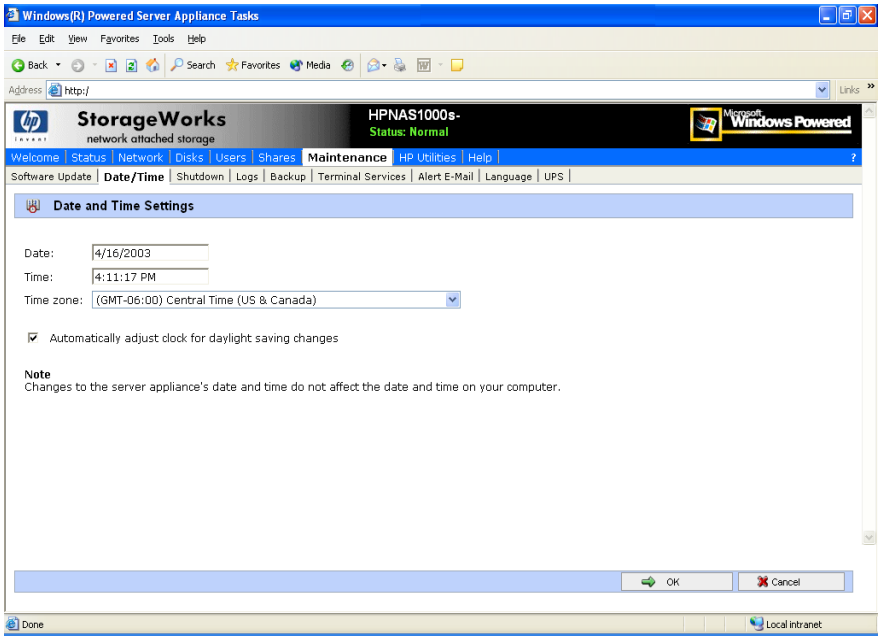
Windows(R) Powered Server Appliance Tasks
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http:/
Links
StorageWorks
network attached storage
HPNAS1000s-
Status: Normal
Microsoft Windows Powered
Welcome Status Network Disks Users Shares Maintenance HP Utilities Help
Software Update Date/Time Shutdown Logs Backup Terminal Services Alert E-Mail Language UPS
Date and Time Settings
Date: 4/16/2003
Time: 4:11:17 PM
Time zone: (GMT-06:00) Central Time (US & Canada)
Automatically adjust clock for daylight saving changes
Note
Changes to the server appliance's date and time do not affect the date and time on your computer.
OK
Cancel
Done
Local intranet

Figure 5: Date and Time dialog box

Shutting Down or Restarting the Server

Caution: Notify users before powering down the system. Both UNIX and Windows NT users can be drastically affected if they are not prepared for a system power-down.

1. From the NAS 1000s WebUI, select **Maintenance**, **Shutdown**. Several options are displayed: **Restart**, **Shut Down**, and **Scheduled Shutdown**.

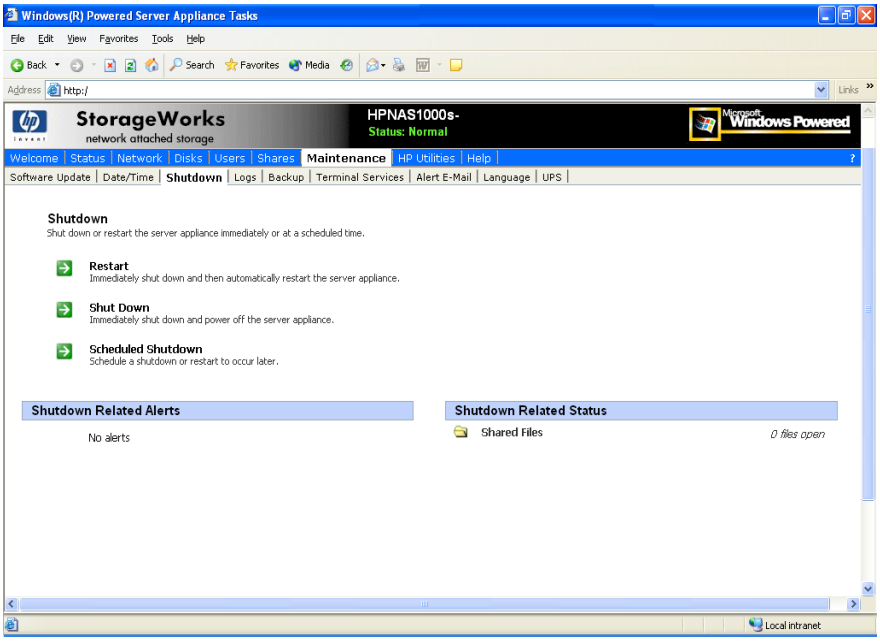
Windows(R) Powered Server Appliance Tasks
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http:/
Links
StorageWorks
network attached storage
HPNAS1000s-
Status: Normal
Microsoft Windows Powered
Welcome Status Network Disks Users Shares Maintenance HP Utilities Help
Software Update Date/Time Shutdown Logs Backup Terminal Services Alert E-Mail Language UPS
Shutdown
Shut down or restart the server appliance immediately or at a scheduled time.
Restart
Immediately shut down and then automatically restart the server appliance.
Shut Down
Immediately shut down and power off the server appliance.
Scheduled Shutdown
Schedule a shutdown or restart to occur later.
Shutdown Related Alerts
No alerts
Shutdown Related Status
Shared Files
0 files open
Local intranet

Figure 6: Shutdown menu

   a. To shut down and automatically restart the server, click **Restart**.
   b. To shut down and power off the server, click **Shut Down**.
   c. To schedule a shutdown, click **Scheduled Shutdown**.

2. Regardless of the choice, a confirmation prompt is displayed. After verifying that this is the desired action, click **OK**. Several status messages are displayed during the shutdown process.

Viewing and Maintaining Audit Logs

A variety of audit logs are provided on the NAS 1000s. System events are grouped into similar categories, representing the seven different logs.

To access the logs from the WebUI, select **Maintenance**, **Logs**. The **Logs** menu is displayed.

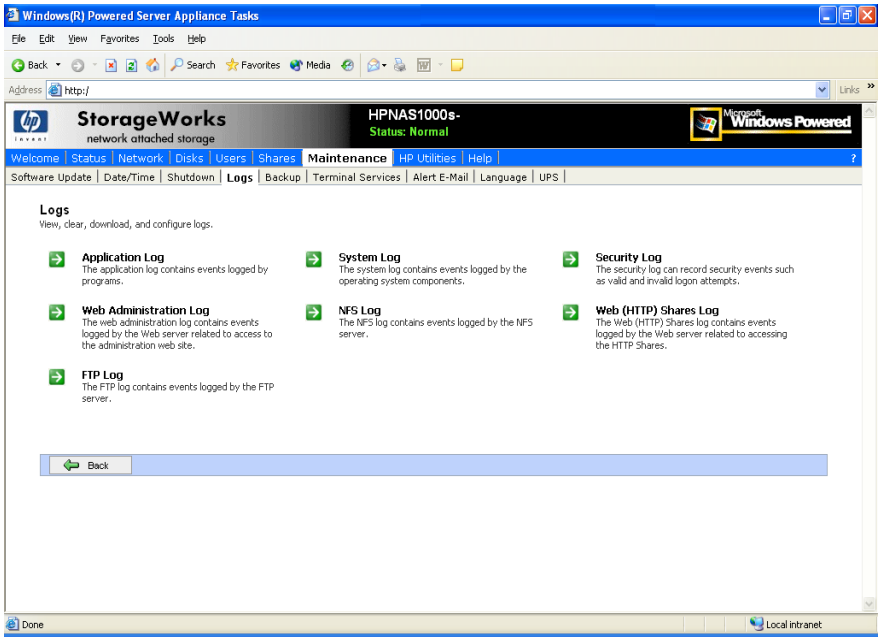
Windows(R) Powered Server Appliance Tasks
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http:/
Links
StorageWorks
network attached storage
HPNAS1000s-
Status: Normal
Microsoft Windows Powered
Welcome Status Network Disks Users Shares Maintenance HP Utilities Help
Software Update Date/Time Shutdown Logs Backup Terminal Services Alert E-Mail Language UPS
Logs
View, clear, download, and configure logs.
Application Log
The application log contains events logged by programs.
System Log
The system log contains events logged by the operating system components.
Security Log
The security log can record security events such as valid and invalid logon attempts.
Web Administration Log
The web administration log contains events logged by the Web server related to access to the administration web site.
NFS Log
The NFS log contains events logged by the NFS server.
Web (HTTP) Shares Log
The Web (HTTP) Shares log contains events logged by the Web server related to accessing the HTTP Shares.
FTP Log
The FTP log contains events logged by the FTP server.
Back
Done
Local intranet

Figure 7: Logs menu

A variety of logs are available and are listed in Figure 7.

Each log has viewing, clearing, printing, and saving options.

Using Terminal Services

Terminal Services is provided in the WebUI to allow for additional remote system administration and the use of approved third-party applications. Backup software and antivirus programs are examples of approved applications.

In addition, Terminal Services is used to access the NAS Management Console of the NAS device.

To open a Terminal Services session from the WebUI, select **Maintenance**, **Terminal Services**. A Terminal Services session is opened. Enter the appropriate password to log on to the server.

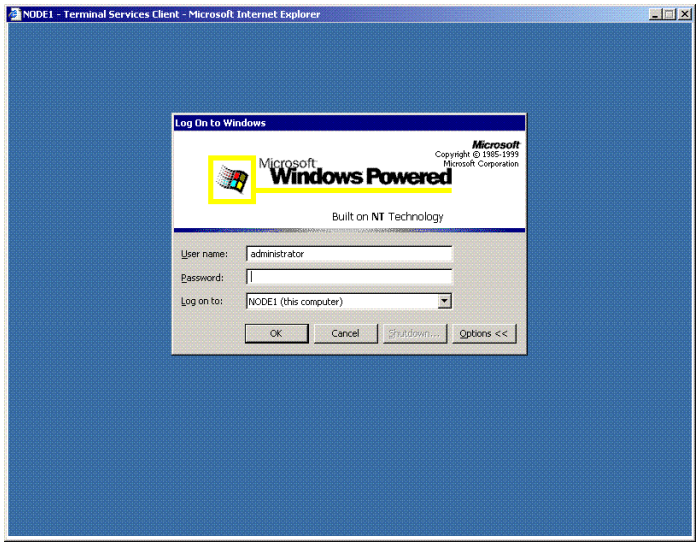

Figure 8: Terminal Services session

Caution: Two open sessions of Terminal Services are allowed to operate at the same time. After completing an application do not use the window close feature ( ) to close that session of Terminal Services. Click on **Start/Log Off Administrator** to exit Terminal Services.

Setting up E-mail Alerts

If desired, the system sends emails of system events to a specified email account. When activated, this feature sends an e-mail whenever system alerts occur.

To activate this option:

1. From the WebUI, select **Maintenance**, **Alert E-mail**. The **Set Alert E-Mail** dialog box is displayed.
2. Select **Enable Alert E-mail**.
3. Indicate the types of messages to be sent.
   - Critical alerts
   - Warning alerts
   - Informational alerts
4. Enter the desired e-mail address in the appropriate boxes.
5. After all settings have been entered, click **OK**.

Updating the Software

To update the software, click on **Software Update** from the **Maintenance** menu. The Software Update Wizard will guide you through selecting, verifying, and updating the desired software.

Changing System Network Settings

Network properties are entered and managed from the **Network** menu. Most of these settings are entered as part of the Rapid Startup process. Settings made from this menu include adding the NAS 1000s to a domain.

Online help is available for these settings. Figure 9 is an illustration of the Network settings menu.

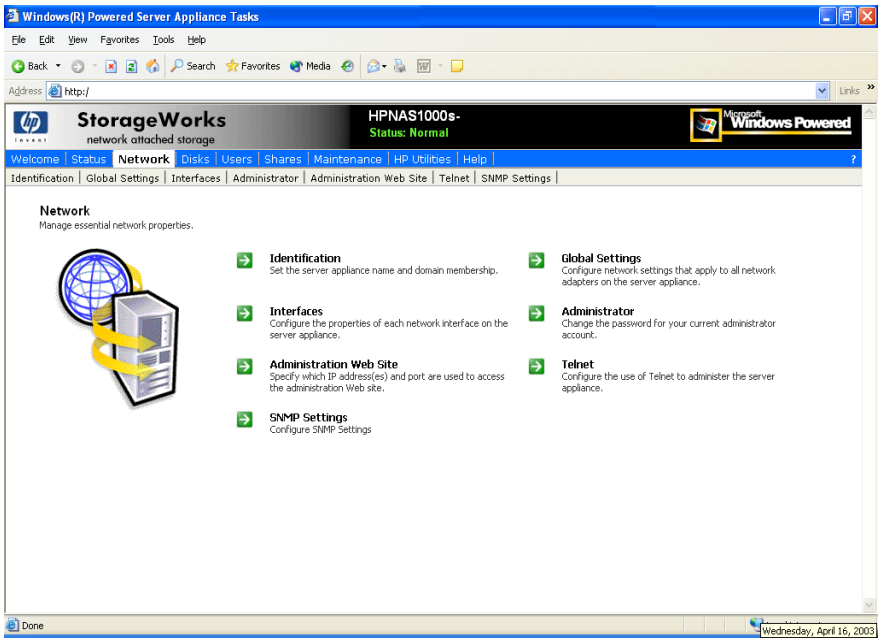
Windows(R) Powered Server Appliance Tasks
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http:/
Links
StorageWorks
network attached storage
HPNAS1000s-
Status: Normal
Microsoft Windows Powered
Welcome Status Network Disks Users Shares Maintenance HP Utilities Help
Identification Global Settings Interfaces Administrator Administration Web Site Telnet SNMP Settings
Network
Manage essential network properties.
Identification
Set the server appliance name and domain membership.
Global Settings
Configure network settings that apply to all network adapters on the server appliance.
Interfaces
Configure the properties of each network interface on the server appliance.
Administrator
Change the password for your current administrator account.
Administration Web Site
Specify which IP address(es) and port are used to access the administration Web site.
Telnet
Configure the use of Telnet to administer the server appliance.
SNMP Settings
Configure SNMP Settings
Done
Wednesday, April 16, 2003

Figure 9: Network menu

Persistent Storage Manager

3

Persistent Storage Manager lets the administrator make replicas, called snapshots, of disks in a matter of seconds. Snapshots enable the creation of multipurpose virtual replicas of production data without having to physically copy the data. They can be used to immediately recover a lost file or directory, to test a new application with realistic data without affecting the "real" data, and to serve as a source of data for backups. Snapshots record data changes on volumes and are thus not a replacement for off-line backups.

This chapter covers the following items:

- Operational Overview
- Data Recovery
- Snapshot (Persistent Image) Considerations
- Accessing Persistent Storage Manager

Operational Overview

Each snapshot is a complete point-in-time representation of the data on the volumes. Each snapshot requires only a fraction of the hard-drive capacity of the original data. PSM does not keep all the data that was ever written. PSM maintains only the data required to maintain a snapshot.

PSM works below the operating system as a Filter Driver at the Volume block level. PSM maintains a library of snapshots, each representing a specific point-in-time. Snapshots can be accessed by users, administrators, or any Windows application, and look just like the familiar file/folder view.

With the first snapshot taken on a target volume, PSM establishes a cache file for that volume within which PSM retains overwritten data required to build a snapshot. The cache file size is based on a percentage of the volume it resides on and is configured through the WebUI; the default is 10 percent. As soon as the first snapshot is taken, PSM starts monitoring all writes on the target volume. When a write request occurs, PSM intercepts and pauses the write, reads the data that is to be overwritten, and saves the data in a Diff Directory within the PSM-specific cache file. After the original data is written to the Diff Directory, the new data is written on the active volume. This process is referred to as "copy-on-write." Only the first write forces a copy-out, subsequent writes to the same data block does not force a new copy-out, unless of course a new snapshot is taken between the initial and subsequent write.

PSM can create and manage up to 250 snapshots system wide. A snapshot can cover several volumes at once with an upper limit of 63 volumes within a single snapshot. However, when reverting from a "grouped" snapshot, the revert is non-selective and it reverts all volumes associated with the "grouped" snapshot.

Reading Snapshots

Users who have been granted access by the NAS Administrator see snapshots as network shares.

A snapshot is a representation of the NAS volume at the time it was created. During the copy-on-write operation, the data to be overwritten is preserved in the PSM Diff Directory. When reading a snapshot, PSM determines if the data has changed, meaning it is located in the Diff Directory, or if it is on the live volume. For data that has changed, PSM inserts the original data, held in the Diff Directory and, where no changes have occurred, PSM reads directly from the live volume.

Creating Snapshots

Creation of snapshots is scheduled through the SAK interface or may be generated by the NAS Administrator as a one-time request. When the command to create a snapshot is issued, PSM begins monitoring the file system looking for a quiescent period. A quiescent period is the amount of time a volume must be dormant before a snapshot is created. The default quiescent duration is five seconds but the NAS administrator may configure this, as can the amount of time PSM should search for this inactivity window. The quiescent period provides sufficient time for completion of writes and for the various software buffers to flush, the premise being that, by the end of the quiescent period, a volume will be produced which is in a stable state meaning that the volume is at rest and in a functional condition ready for users to access. If the volume is captured in a stable state, then that volume, or files and folder contained in the volume, will be returnable in a stable state or "useable condition" to users.

Following the quiescent period, PSM creates the snapshot.

PSM Snapshot Attributes

When creating PSM snapshots there are three basic attributes which affect the life and consistency of the snapshot. They are Read-only, Read/write and Always Keep. Read-only should be used to enforce the integrity of a snapshot so that changes can not be made to. Read/Write can be used in instances where test data is useful, such as developers altering a test website. Always Keep is useful when a snapshot needs to live indefinitely. These attributes are described in detail below.

Read Only

The default setting is for PSM to create "READ ONLY" snapshots which prohibits any modification to the snapshot - this is the most common parameter for snapshots. A READ ONLY snapshot allows users, who have been granted access, to view, open and save a copy of any file represent in the snapshot. The properties of a READ ONLY snapshot may be modified by the NAS Administrator to READ/WRITE or ALWAYS KEEP.

Read/Write

The READ/WRITE attribute may be assigned at the time of creation or the NAS Administrator may at any time change the attribute of any snapshot. READ/WRITE snapshots provide some unique capabilities to PSM.

READ ONLY snapshots changed to READ/WRITE snapshots and then modified return the data represented in the snapshot to the way it was originally, effectively acting as an UNDO.

Other applications for READ/WRITE snapshots: CFOs and auditors can run trial balances to accounting systems without affecting the actual systems. Prototyping, a new version of a program, can be installed in a READ/WRITE snapshot and its compatibility within the system tested with no adverse effects to the primary system.

Always Keep

ALWAYS KEEP snapshots are treated as untouchable by PSM. In a cache file fill situation PSM will cease writing to the cache file to avoid deleting or corrupting an ALWAYS KEEP snapshot. A "disk full" error will be returned to the user. ALWAYS KEEP allows the administrator to set some milestones that are not subject to the automatic deletion routines.

Automated Snapshot Deletion

PSM has a snapshot weighting system (low to highest) that helps set the priority of the snapshot. This weighting combined with the age of the snapshot determines the order by which it is deleted by PSM when the cache file fills up.

A key fact to consider is that PSM provides Primary Data Protection automatically. Once set up, PSM continues to provide Data Protection generating new scheduled snapshots or deleting older snapshots with little or no input required from system administrators.

Data Recovery

File/Folder/Volume Recovery

PSM facilitates instant data recovery from the stored on-line images. Individual files, groups of files, folders, groups of folders or complete volumes can be restored. Recovering the data can be accomplished by the NAS Administrator or the NAS Administrator can give individual users access to their data for that purpose through file share access over the network.

Security rights and privileges, as well as file and directory attributes, remain in effect as they were at the time the snapshot was created.

Snapshots and Drive Defragmentation

A drive defragmenter attempts to consolidate files on a drive by reading various parts of the files and rewriting them to become contiguous on the drive. When volumes are created they are initially contiguous as possible on the underlying storage units (RAID arrays and LUNs). If defrag utilities are used on volumes where snapshots exists, snapshots would grow as the defrag utility moves blocks from one part of the disk to another. PSM disables defrag on volumes that have current running snapshots to prevent the unnatural growth of the snapshot.

PSM (current versions) is fully compatible with the Windows 2000 system file defrag utility. On drives upon which snapshots are not installed or are not active, the defrag utility runs without interruption. If snapshots are active, by design, the drive is automatically marked as unavailable for defragmentation. In operation, the utility works as designed - providing defrag on volumes where it is allowed and omitting drives with active PSM Images. There is no user intervention required. This is consistent with the defragmentation handling of system and special files and is officially supported by the Microsoft defrag API. In the rare case when an existing volume requires defrag, disable scheduled snapshots, delete all snapshots on the volume and defrag the volume. When defrag completes, re-enable scheduled snapshots. Defrag is only effective when there are NO snapshots active on the volume being defragged.

Note: Defragmentation can not be performed if snapshots exist. To defragment a disk, first delete the snapshots. Drive defragmentation only operates on volumes formatted with a 4 KB or smaller allocation size. HP recommends larger allocation cluster sizes to improve performance.

PSM and Backup

Because snapshots are quick to create, it is possible to capture a coherent view of the volume data with little or no application downtime. Lack of application downtime removes the traditional backup window or the amount of time taken to back up to offline media. While many applications must be shut down to capture an accurate backup, snapshots capture a point in time view of the data that can be used as the source of backup data. Applications can continue processing against the volume. Therefore, applications may only have to be interrupted for a few seconds during the snapshot process.

Caution: Snapshots are not a replacement for reliable, periodic data backup. If free cache space becomes critical, snapshots are automatically deleted. See the "Automated Snapshot Deletion" section. In addition, snapshots are a short term convenience and may reside on the same physical drives as the data. If something happens to the data drives, the snapshots are also affected. Read Appendix A for suggestions on how to back up the NAS device.

Although snapshots provide a mechanism for backup that does not require downtime, there are some considerations that should be given when performing backup and restore of a system using snapshots. HP recommends you review this section prior to establishing backup and restore policies. Backup and Restore programs are not trivial applications. As such they require effort to set up and use effectively. Given the nature of these products, it is critical that any backup and recovery plan be thoroughly tested before use on a live system.

Be sure to use a backup program that is PSM aware and has been certified for operation with PSM. This is especially true for open file options, system agents, and disaster recovery.

For backup:

- For base volumes that have snapshots in use or when backing up snapshots, archive bit resets and incremental backups should not be used. Archive bit resets are recorded as a change to the data and can fill the cache file with changes. Incremental backups make use of the archive bit set as well. Note if the snapshot is set to read only the backup will also fail.
- Be careful in the selection of folders, since snapshot folders provide a view into the data that can result in the backup of multiple views of the data. Forcing the backup to grow based on the number of snapshots in use.
- Junction points should be turned off to prevent the traversal of multiple snapshot directories of base volume backups.
- Junction points should be turned on when backing up a single snapshot. Be sure to pick the single snapshot and not the root folder. Selecting the root folder will cause multiple snapshot backups.

For restore:

- Delete all active snapshots as the restore will cause the cache file to grow.
- Select only the files representing the data of the volume and not the *.psm files.
- Be sure to restore to the root of the target volume.
- Restoration of operating system partitions does not restore the registry hive. System state backups should be utilized in these instances.

Snapshots Performance Impact

When using snapshots, performance of the disk may be affected, depending on the rate that data is changing and the number of snapshots kept for each disk. Read performance of the disk remains constant, regardless of the presence of snapshots. Read performance of the snapshot is identical to that of the disk. Write performance, however, may vary. PSM creates minimal additional I/O overhead which is limited to writes. The copy-on-write process adds one read (the write is paused to read the old data) and one write (the old data is written to the Diff Directory file) to each write system request. This only affects each initial write to a disk area that has a snapshot running on it. Copy out is not performed on subsequent writes to the same disk block, so write performance is unaffected after the initial write to each block.

Predicting the exact effect of snapshots on any particular disk is difficult, because several variables are involved. These variables include the type of applications accessing the data and the rate of change of the files on the disk. When a high percentage of writes is made to the same area, as when a file is constantly rewritten, the effect is called write locality. Disks with high write locality experience less performance degradation due to snapshots.

Recovering Snapshots after a System Restore or System Loss

The NAS 1000s ships with a Quick Restore DVD in case the server must be restored to its factory default state. If the primary operating system becomes corrupted and unaccessable, registry information for existing snapshots are lost. Volume data remains unaltered and accessable using the secondary OS. However, the snapshots are invalid. Even though all snapshot folders and cache files exist on the system volumes, the snapshots are not accessible to PSM in the secondary OS, and are orphaned. At this time, the user should backup all data by booting using the secondary OS and then restore the system to it's factory default state using the included Quick Restore DVD.

Caution: Performing a quick restore prcedure using the Quick Restore DVD will delete all data on all drives in the system.

Granule Size Update Utility

PSM ships with a utility for adjusting the Granule size of the snapshots. Granules determine the largest cache size that can be managed by PSM. The default setting in the PSM product that ships on the NAS 1000s is 64 K. This setting will allow for up to 1 TB of data to be written to the cache file. In order to gain greater cache file space, the granule size will need to be adjusted. The following table provides an overview of the addressable storage space and maximum cache size of each Granular size.

Table 2: Adjusting Granule Size

Granule Size	Largest Cache Size
64K granule	1 TB
128K granule	2 TB
256K granule	4 TB

When considering the granule size the following rules should be observed.

- Before altering the granule size, all snapshots should be removed from the target system.
- Cache File size is fixed as in the above table and the limit applies to the sum total of all cache files system wide.
- Granule size affects only the block size utilized for each change that is written to the cache files. Regardless of the setting, there is approximately 15.6 million blocks available for storing snapshot information system wide other system limitations may further limit this maximum such as memory consumption.
- If the changes occur in different underlying blocks, more blocks of larger space could get written for any set of changes, versus if the changes all occur in the same block. Therefore increased granule size does not necessarily lead to increased coverage for changes on the originating volumes. In theory, larger blocks should lead to fewer blocks consumed to record the original data due to write locality.
- Highly fragmented disk space could lead to increased separate cache writes and more consumption of the maximum available number of blocks system wide.
- Setting the value too low will limit the available space for cache file writes. For example, a 10 TB system undergoing change could only experience a 10 % change in original data if the granule size is set to 64 KB, assuming all of the changes fit neatly into the 64KB blocks.
- PSM now supports the PSM granule sizes of 64K, 128K, 256K with 64K as the default. This will allow for cache file to be 1TB, 2TB, and 4TB respectively. The program GRANSIZE.EXE, available in the directory c:\winnt\system32\serverappliance, is provided for setup - By increasing the granule size, PSM can be better suited to support very large terabyte systems. The command provides an error message if there are running snapshots on the system. Typing GRANSIZE ? will display the current granule size in use in the system. Typing just GRANSIZE will display the command usage. The command must be executed from a command prompt while residing in the directory stated above.

- When changing to a larger granule for systems, thus allowing for larger cache file sizes and accommodating larger amounts of storage, users should lower their percentage of volume space for the cache file. For example, if the percent is 30 and the supported amount of space in the system is 20 TB, then the cache file limit of 4 TB would get exceeded. Should the limit get exceed, PSM will issue an "Out of Memory" error in the event log and the WebUI status page. If the limit is exceeded, the cache file must be removed or reduced in size prior to system restart using either the clearvol command or by reducing the percent cache size under volume settings.

Clearing the Cache File from the System

The PSM interface allows the user to set the cache file to any percentage from 1 - 70 percent but it will not allow the deletion of the cache file in its entirety. It is possible to delete these files but the process must be done from the command prompt either through Terminal Services or from the NAS console. To delete the PSM cache files and cache directories the following command: CleanVol.exe Vol: must be performed for each existing volume where the cache file is no longer desired. The command may be found in *c:\winnt\system32\serverappliance*. Typing cleanvol will display the command usage. Prior to these steps the snapshots on the target volume need to be deleted as well or "access denied" error will be returned.

Re-extending Volumes from Old Snapshots

Volumes based on dynamic disks may be extended utilizing LDM. Corresponding snapshots can exist at points in time prior to the extension and after the extension. If a re-extended volume containing snapshots of the pre-extended volume is reverted, the re-extended area of the disk will be unusable. To reclaim this space, make sure the included utility reextend.exe is executed after reverting from a snapshot of the pre-extended volume.

This utility is available in the directory *c:\winnt\system32\serverappliance* and must be executed either through terminal services or at the NAS console.

Usage of this utility is available by typing `reextend -?`.

This program will extend a volume back to its original size after a restore operation of a smaller volume from a snapshot.

Volume Display in Persistent Storage Manager

PSM fully supports the use of all Logical Disk Manager storage elements this includes basic, dynamic, partitions, extended partitions, and volumes provided they are formatted as NTFS when created. PSM makes use of two items when displaying storage elements in the UI. These include the volume label and the GUID representing that volume or partition. In several web pages, the information displayed is limited with regard to the identification information and the volume label is essentially all that can be viewed. It is therefore important that volume labels be identifiable by the user to avoid confusing one volume over another. By default, Local Volume, followed by the drive letter is displayed, for mount points the GUID is displayed. This label should be updated to reflect a unique label either during volume/partition creation in LDM or post volume/partition creation via File Explorer and the properties tab of the target drive.

Persistent Storage Manager Storage Limitations

The version of PSM included in the NAS 1000s is currently designed to work with 10 TB of storage with the ability to take 250 snapshots The NAS 1000s is capable of addressing 1TB using the fully populated system and 250 GB Drives. PSM will continue to function with larger systems but the snapshot coverage should only encompass 10 TB worth of storage. There are no safeguards to prevent the use of storage greater than 10 TB. HP is currently working with CPD to address this storage limitation. Please check the HP website for updates reagarding this suppport.Accessing Persistent Storage Manager

To access PSM, from the **WebUI Welcome** screen, select **Disks**, then **Persistent Storage Manager**.

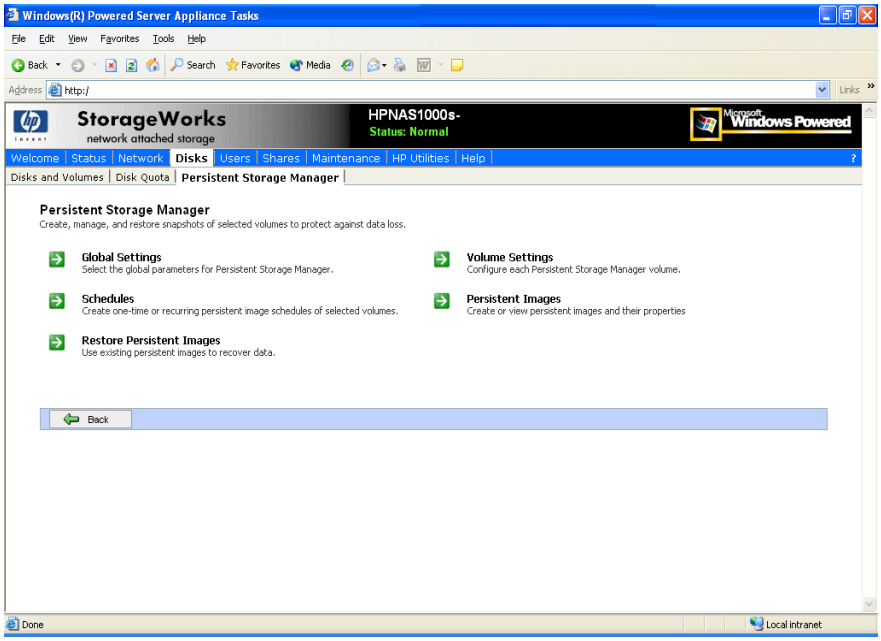
Windows(R) Powered Server Appliance Tasks
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http:/
Links
StorageWorks
network attached storage
HPNAS1000s-
Status: Normal
Microsoft Windows Powered
Welcome Status Network Disks Users Shares Maintenance HP Utilities Help
Disks and Volumes Disk Quota Persistent Storage Manager
Persistent Storage Manager
Create, manage, and restore snapshots of selected volumes to protect against data loss.
Global Settings
Select the global parameters for Persistent Storage Manager.
Volume Settings
Configure each Persistent Storage Manager volume.
Schedules
Create one-time or recurring persistent image schedules of selected volumes.
Persistent Images
Create or view persistent images and their properties
Restore Persistent Images
Use existing persistent images to recover data.
Back
Done
Local intranet

Figure 10: PSM Main screen

Global Settings

From the **Global Settings** screen you can control the overall environmental settings for Persistent Storage Manager. Some options will be disabled if there are already active snapshots.

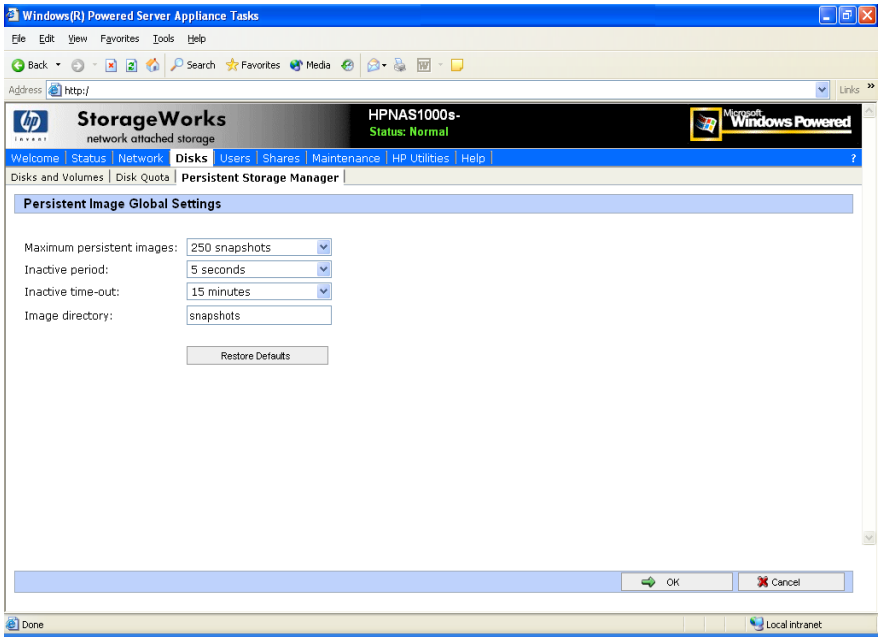

Figure 11: Global settings

Maximum Persistent Images

This option determines the maximum number of active Persistent Images (snapshots). PSM will support a maximum of 250 snapshots per server. The size of the cache file will determine the actual amount each server can hold.

If the creation of a new snapshot would cause the maximum number to be exceeded, the system will delete the oldest existing persistent image according to the deletion heuristics established by the user.

Inactive Period

This option specifies the amount of time a volume must be dormant before a snapshot is created. Before starting a snapshot, the system will wait for the volume being imaged to become inactive. The default value will allow systems to start an image with a consistent file set and a minimal time-out. Administrators can change this value for system optimization. Reducing the inactive period will allow you to create snapshots even on busy systems, but with possible synchronization problems within applications which are concurrently writing to multiple files.

Inactive time-out

This option specifies how long the server should try to create a snapshot. A snapshot will not begin until a period of relative inactivity set by the Inactive period has passed. If an interval passes that is longer than the Inactive time-out period, the snapshot will not be created and a notice generated to the system event log.

Image directory

This option specifies the root directory used for the snapshot. Each snapshot appears as a subdirectory of the volume that is being imaged. The entire content of the volume as it existed at the moment the snapshot was created will appear under this directory.

Restore Defaults

The **Restore Defaults** button will reset the system defaults.

Volume Settings

From the PSM screen select **Volume Settings**. From the **Volume Settings** screen you can view the Persistent Storage Manager attributes for each volume and change volume settings using the **Configure** button in the **Tasks** list.

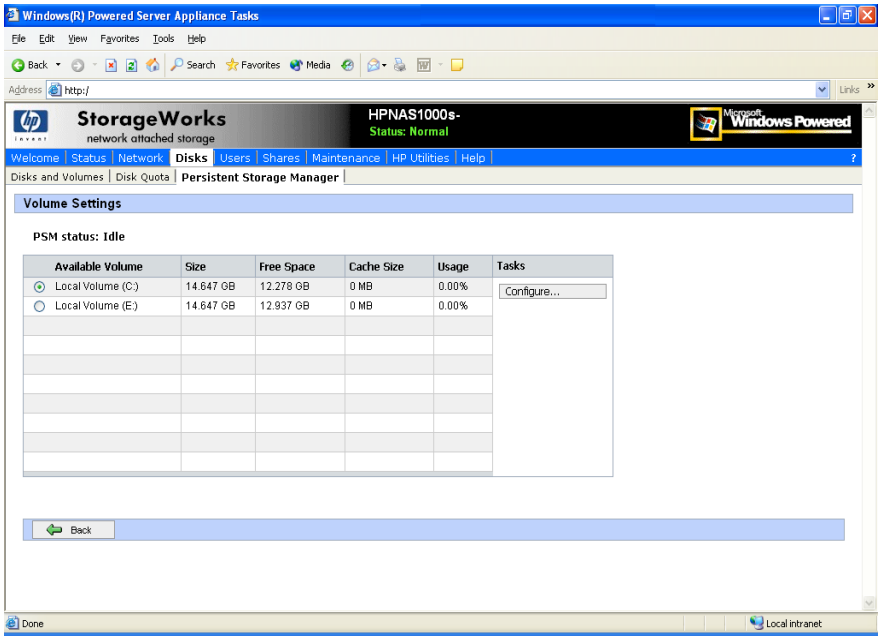
Windows(R) Powered Server Appliance Tasks
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http:/
StorageWorks
network attached storage
HPNAS1000s-
Status: Normal
Microsoft Windows Powered
Welcome Status Network Disks Users Shares Maintenance HP Utilities Help
Disks and Volumes Disk Quota Persistent Storage Manager
Volume Settings
PSM status: Idle
Available Volume Size Free Space Cache Size Usage Tasks
Local Volume (C:) 14.647 GB 12.278 GB 0 MB 0.00%
Local Volume (E:) 14.647 GB 12.937 GB 0 MB 0.00%
Configure...
Back
Done
Local intranet

Figure 12: Volume settings

Available Volume

This field lists all of the volumes that can support snapshots. You can select the volume you want to configure.

Size

This column displays the size of the volume.

Free Space

This column displays the available storage size of the volume.

Cache Size

This column specifies the amount of space allocated to the cache file. Increasing this value will allow more and larger snapshots to be maintained.

Usage

This column displays the current cache file use as a percentage of the cache size.

Volume Configuration Settings

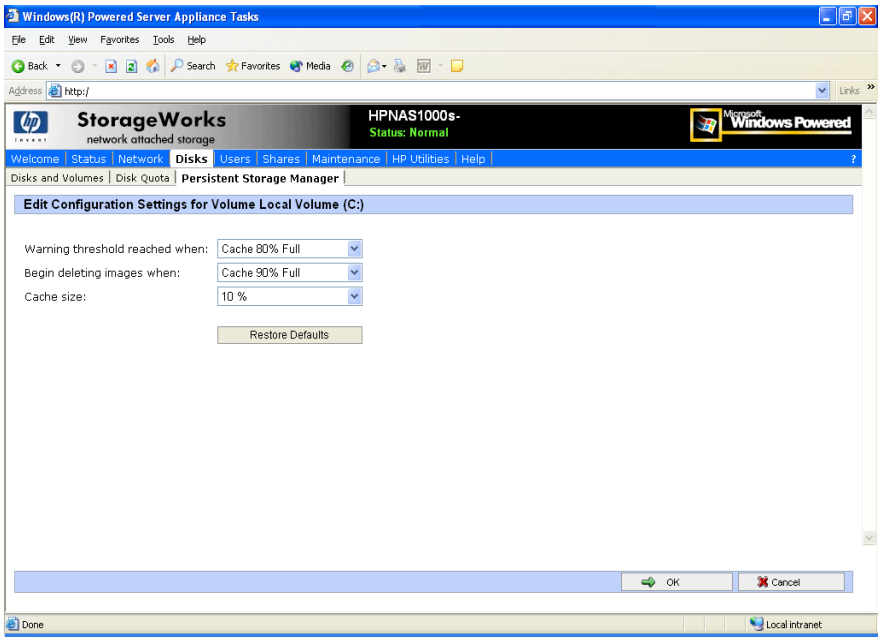

Figure 13: Volume configuration settings

Click **Configure** from the Volume Settings to modify the various aspects of the PSM volume attributes. Some of the fields will appear read-only if there are active snapshots. The **Restore Defaults** button will re-establish the system defaults. If it is desired to remove the cache files all together the *CLEANVOL.EXE* can be used to remove them; see the section on clearing the cache file. Also note the section on granular size in this chapter, prior to updating the percent reserved for cache size. The default value is 10 percent.

Note: Changing the values for the cache size can result in cache files that exceed the maximum cache file based on the current granule size. If the limit is exceeded "out of memory" notices appear in the event log and the WebUI status page when the first snapshot utilizing that cache file is taken. The snapshot will fail to create but the cache file is built regardless. It is important to reduce the cache file size via the above screen or clean the cache files prior to the restart of the NAS system if an oversized cache file is created.

Warning threshold reached when

This option defines the percentage of cache space which, when consumed, will trigger warning messages to the system event log.

Begin deleting images when

This option defines the percentage of cache space which, when consumed, will trigger the automatic deletion of the oldest snapshot on the system. Automatic snapshot deletions are recorded in the system log.

Cache size

This option specifies the amount of space allocated to the cache file. Increasing this value will allow more and larger snapshots to be maintained. Make sure that adequate space is available on the drive where snapshots are stored.

Schedules

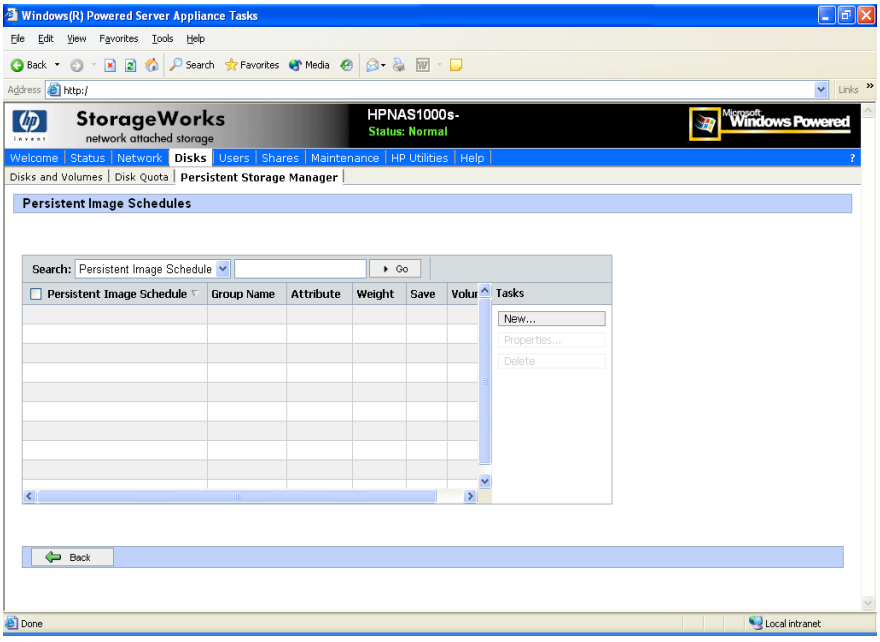

Figure 14: Persistent Image Schedules

The **Persistent Storage Manager Schedules** page displays a list of scheduled snapshots and associated tasks.

Each scheduled snapshot contains information such as its scheduled time, day, frequency, starting date, and group name.

Schedules screen allows you to create new schedules, delete existing schedules, and edit schedule properties.

Create a New Schedule

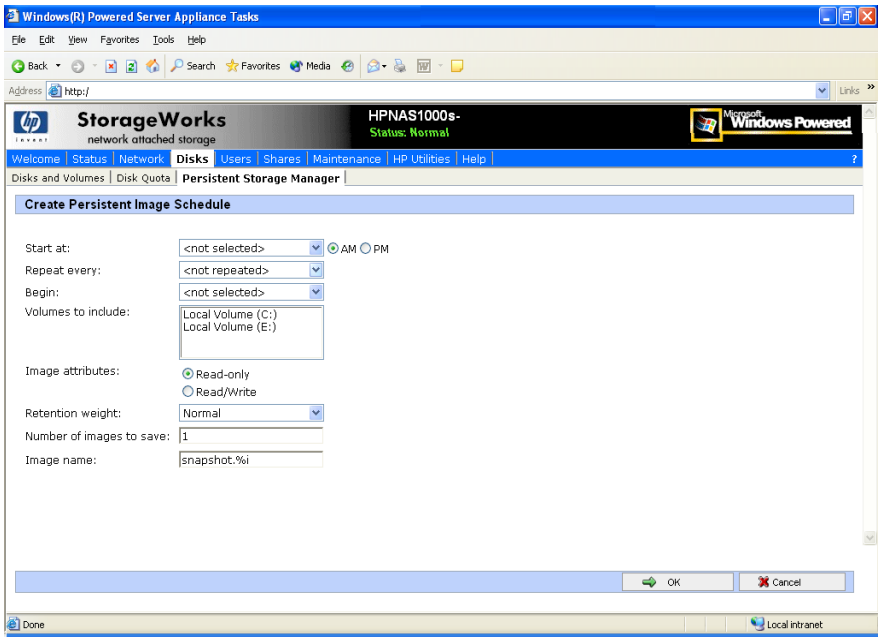

Figure 15: Create Persistent Image Schedule

To create a new schedule, you must supply a starting time, repeat period, starting day, volume, and the number of snapshots to make available to users.

To add a snapshot to the schedule:

1. Select **Schedules** from the **PSM Main** screen.
2. In the **Tasks** list, select **New**.
3. Select the parameters you want for the schedule.
4. Click **OK**.

Editing Persistent Image Schedule Properties

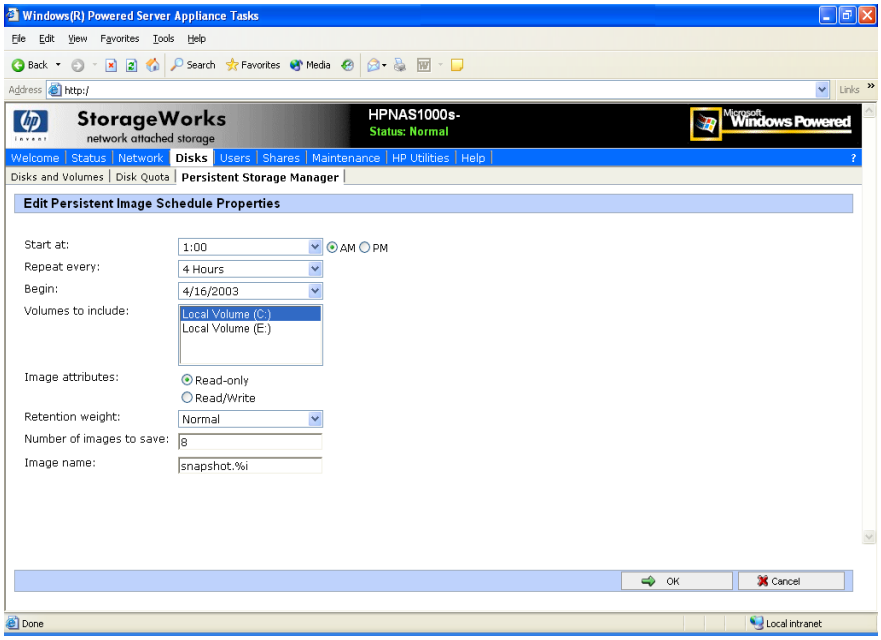

Figure 16: Edit schedule properties

To edit persistent image schedule properties:

1. Select **Schedules** from the **PSM Main** screen.
2. In the **Tasks** list, select **Properties**.
3. Select the changes you want to make to the schedule.
4. Click **OK**.

Deleting a Persistent Image Schedule

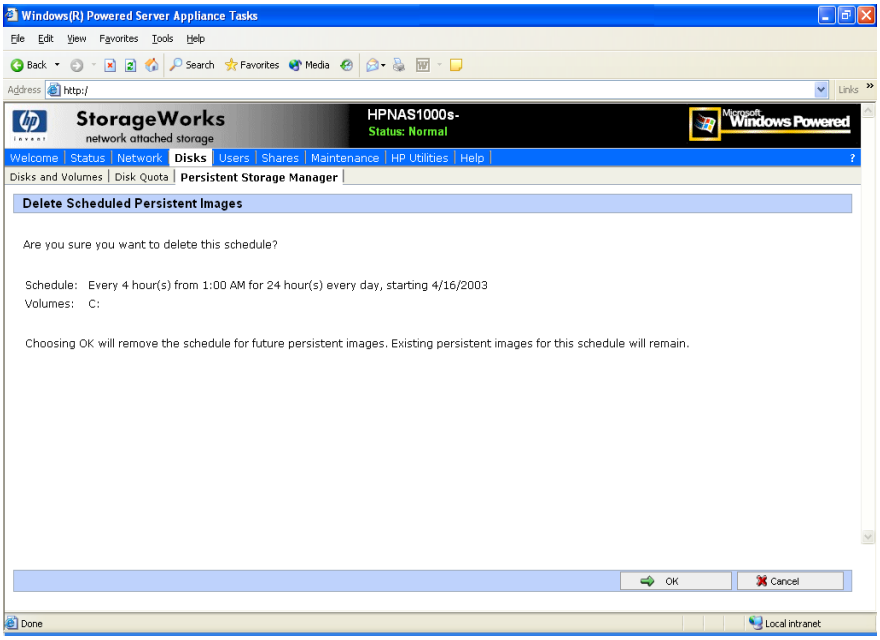
Windows(R) Powered Server Appliance Tasks
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http:/
Links
StorageWorks
network attached storage
HPNAS1000s-
Status: Normal
Microsoft Windows Powered
Welcome Status Network Disks Users Shares Maintenance HP Utilities Help
Disks and Volumes Disk Quota Persistent Storage Manager
Delete Scheduled Persistent Images
Are you sure you want to delete this schedule?
Schedule: Every 4 hour(s) from 1:00 AM for 24 hour(s) every day, starting 4/16/2003
Volumes: C:
Choosing OK will remove the schedule for future persistent images. Existing persistent images for this schedule will remain.
OK
Cancel
Done
Local intranet

Figure 17: Delete scheduled images

To delete a persistent image schedule:

1. Select **Schedules** from the **PSM Main** screen.
2. Select the schedule you want to delete.
3. In the **Tasks** list, select **Delete**.
4. Click **OK**.

Persistent Image and Group Information

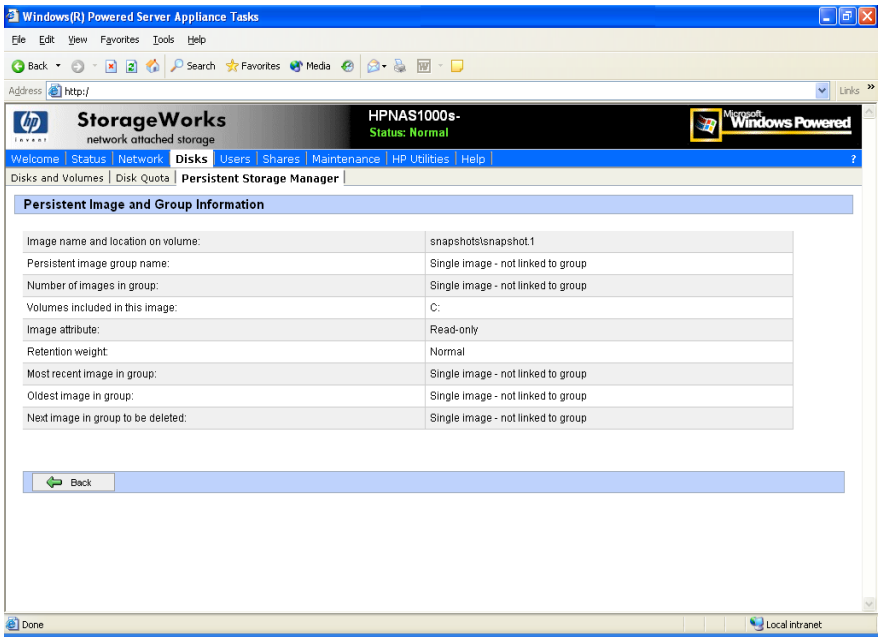
Windows(R) Powered Server Appliance Tasks
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http:/
Links
StorageWorks
network attached storage
HPNAS1000s-
Status: Normal
Microsoft Windows Powered
Welcome Status Network Disks Users Shares Maintenance HP Utilities Help
Disks and Volumes Disk Quota Persistent Storage Manager
Persistent Image and Group Information
Image name and location on volume: snapshots\snapshot.1
Persistent image group name: Single image - not linked to group
Number of images in group: Single image - not linked to group
Volumes included in this image: C:
Image attribute: Read-only
Retention weight: Normal
Most recent image in group: Single image - not linked to group
Oldest image in group: Single image - not linked to group
Next image in group to be deleted: Single image - not linked to group
Back
Done
Local intranet

Figure 18: Persistent Image and Group Information

After a snapshot is created from the schedule you specify, it becomes a member of an image group. The **Persistent Image and Group Information** page can be accessed by selecting the desired snapshot and clicking **Details** on the **Persistent Images to Restore** screen. The screen displays the following information about the image group:

Image name and location on volume

This field displays the name of the image and its path.

Persistent image group name

This field displays the name assigned to this group.

Number of images in group

This field displays the maximum number of images that can be included in the group.

Volumes included in this image

This field displays each volume included in the image.

Image attributes

This field displays the read-only or read/write attribute of the image.

Retention weight

This field displays the relative retention weight of the image.

Most recent image in group

This field displays the date and time of the image most recently added to the group.

Oldest image in group

This field displays the chronologically oldest image in the group.

Next image in group to be deleted

This field displays the date and time of the image that will be deleted next so the system can stay within the saved images limit.

Managing Persistent Images

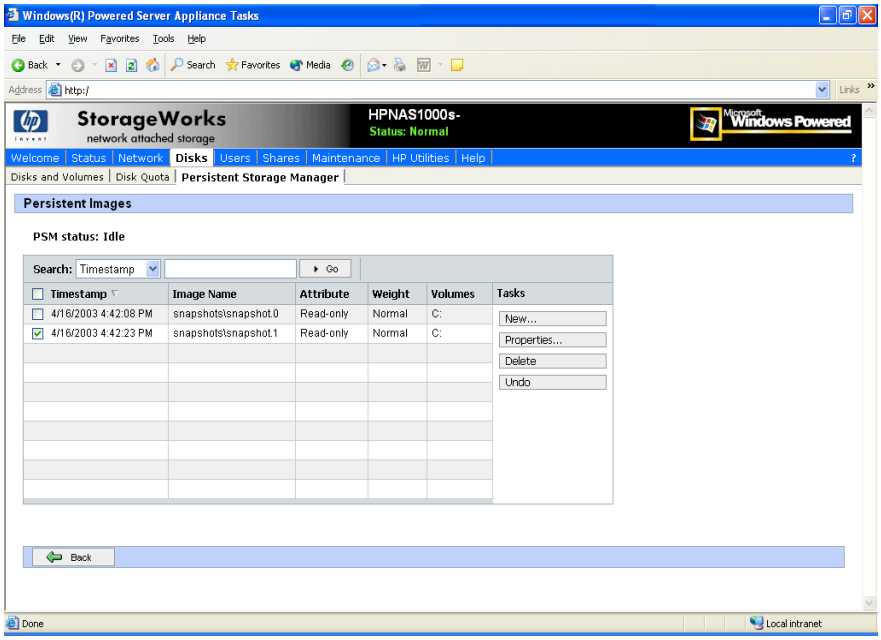

Figure 19: Managing persistent images

The **Persistent Images** page displays active persistent images. Each entry identifies the date and time the snapshot was created, the read-only or read/write attribute, the preservation weight, and the volume it preserves.

To manage snapshots:

1. From the **PSM Main** screen select **Persistent Images**.
2. Select the snapshot you want.

3. Choose one of the following tasks:
   a. Choose **New** to create a new snapshot.
   b. Choose **Properties** to view or change the image read/write attribute or retention weight.
   c. Choose **Delete** to delete the image from the system.
   d. Choose **Undo** to undo changes to a read/write image.

Creating a New Persistent Image

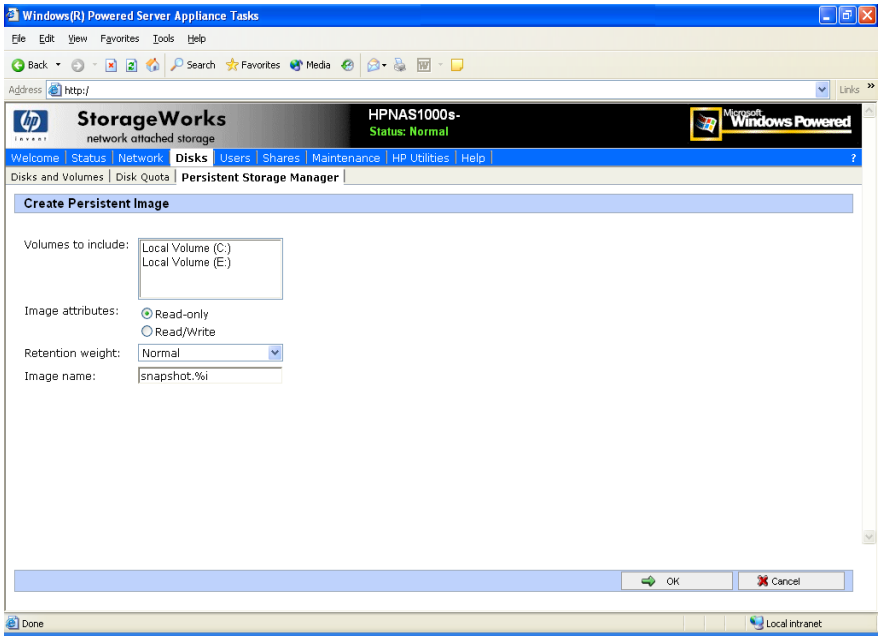

Figure 20: Create new persistent image

Snapshots may be created directly through the **Persistent Images** page. You can also use the **Schedules** page to schedule future or recurring snapshots. To create a new snapshot:

1. From the **PSM Main** screen select **Persistent Images**.
2. In the **Tasks** list, choose **New**.
3. In the **Volumes to include** list, choose volumes to be included in the image.
4. Select the **Read-only** or **Read/Write** button.
5. Select a retention weight from the **Retention weight** list.
6. Type the image name in the Image name box.
7. Choose **OK**.

Deleting a Persistent Image

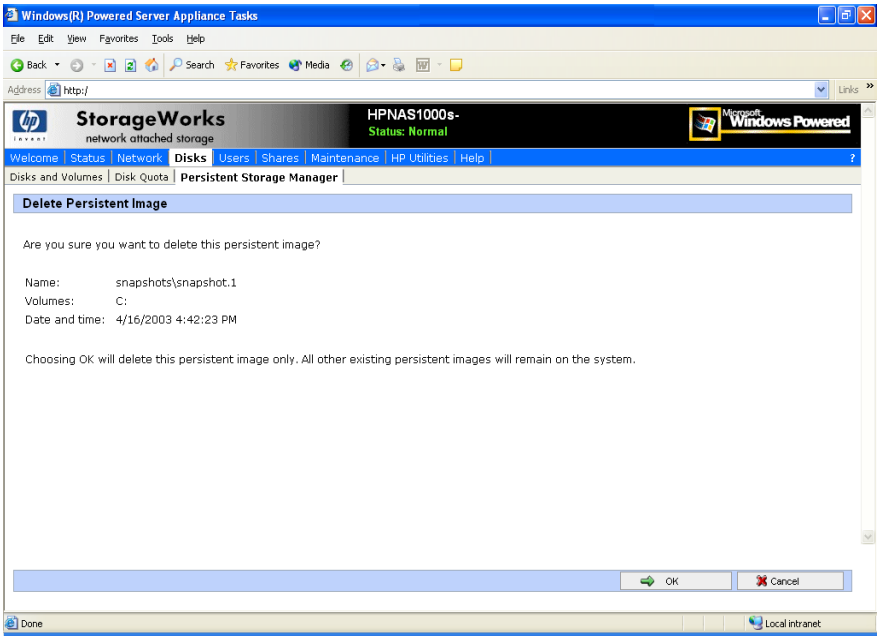
Windows(R) Powered Server Appliance Tasks
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http:/
Links
StorageWorks
network attached storage
HPNAS1000s-
Status: Normal
Microsoft Windows Powered
Welcome Status Network Disks Users Shares Maintenance HP Utilities Help
Disks and Volumes Disk Quota Persistent Storage Manager
Delete Persistent Image
Are you sure you want to delete this persistent image?
Name: snapshots\snapshot.1
Volumes: C:
Date and time: 4/16/2003 4:42:23 PM
Choosing OK will delete this persistent image only. All other existing persistent images will remain on the system.
OK
Cancel
Done
Local intranet

Figure 21: Delete Verification

To delete a persistent image:

1. From the **PSM Main** screen select **Persistent Images**.
2. Select the snapshot you want to delete.
3. In the **Tasks** list, choose **Delete**.
4. Choose **OK**.

Editing Persistent Image Properties

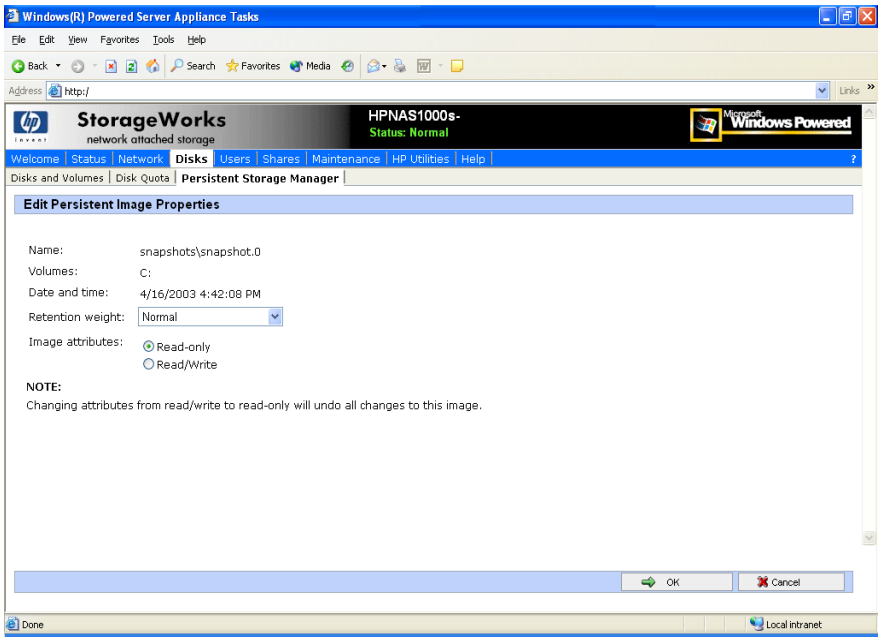

Figure 22: Edit Persistent Image Properties

You can change properties such as the read-only attribute or preservation weight of an image.

To edit persistent image properties:

1. From the **PSM Main** screen select **Persistent Images**.
2. In the **Tasks** list, choose **Properties**.
3. Select a retention weight from the **Retention weight** list.
4. Select the **Read-only** or **Read/Write** button.
5. Choose **OK**.

Undo Persistent Image Changes

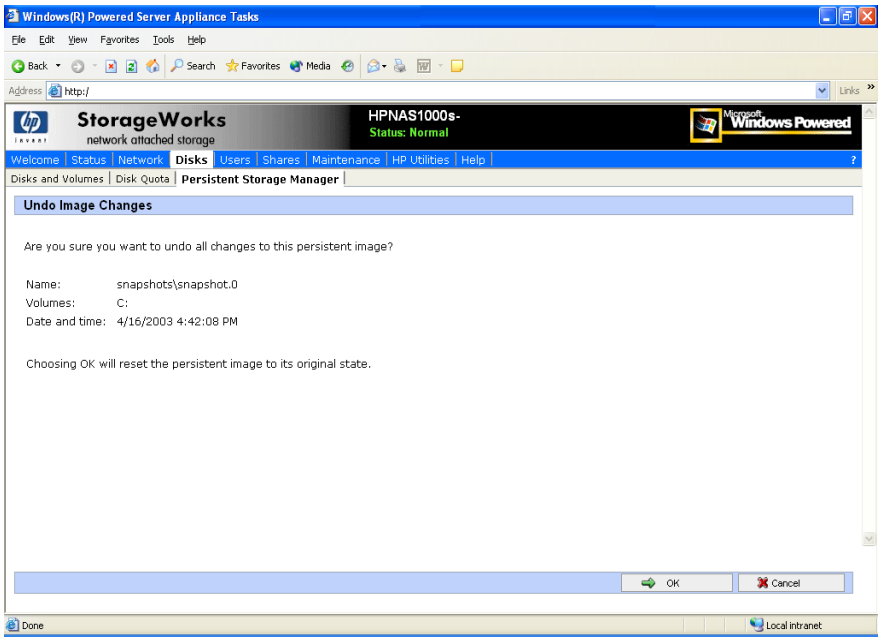
Windows(R) Powered Server Appliance Tasks
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http:/
Links
StorageWorks
network attached storage
HPNAS1000s-
Status: Normal
Microsoft Windows Powered
Welcome Status Network Disks Users Shares Maintenance HP Utilities Help
Disks and Volumes Disk Quota Persistent Storage Manager
Undo Image Changes
Are you sure you want to undo all changes to this persistent image?
Name: snapshots\snapshot.0
Volumes: C:
Date and time: 4/16/2003 4:42:08 PM
Choosing OK will reset the persistent image to its original state.
OK
Cancel
Done
Local intranet

Figure 23: Undo Image Changes

After you create a read/write snapshot, you can make changes to the image, for example, you can modify files in the image, add new files, or delete existing files. If you make a change to an existing image and later want to revert to the original file contents, you can use the following procedure to restore the original snapshot.

To undo snapshot changes:

1. From the **PSM Main** screen select **Persistent Images**.
2. Select the snapshot you want to restore to its original state.
3. In the **Tasks** list, choose **Undo**.
4. Choose **OK**.

Restoring an Image

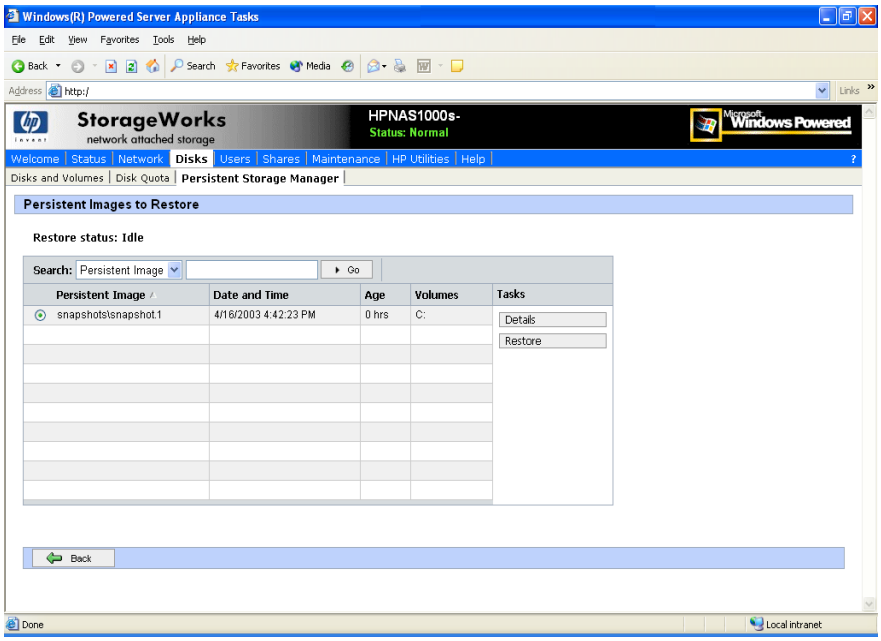

Figure 24: Images available to restore

The **Persistent Images to Restore** page displays a list of all snapshots. You can choose to view an image or restore your server appliance to an image you have previously created.

To restore a snapshot:

1. On the PSM Main screen select **Restore Persistent Images**.
2. Select the snapshot you want to restore.
3. Choose **Restore**.

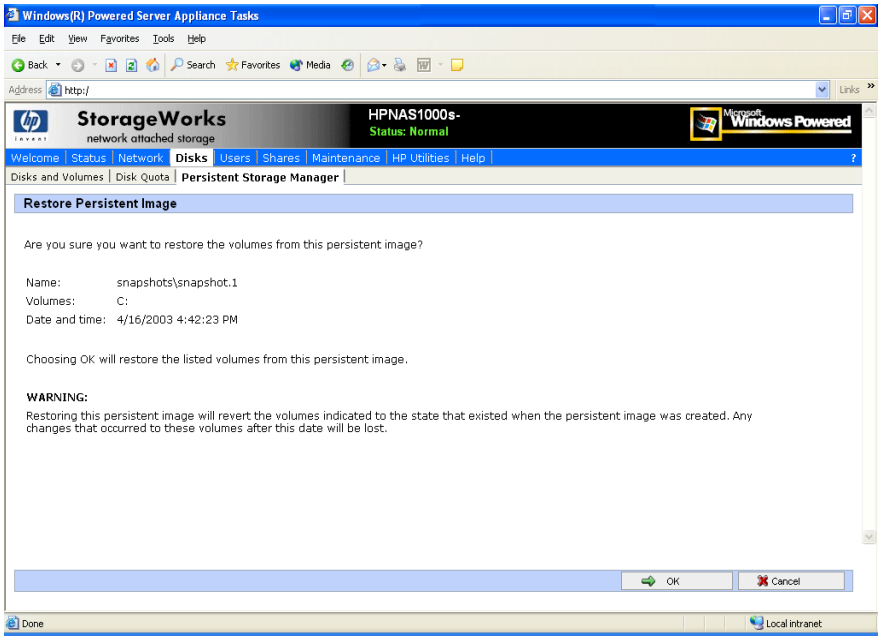
Windows(R) Powered Server Appliance Tasks
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http:/
Links
StorageWorks
network attached storage
HPNAS1000s-
Status: Normal
Microsoft Windows Powered
Welcome Status Network Disks Users Shares Maintenance HP Utilities Help
Disks and Volumes Disk Quota Persistent Storage Manager
Restore Persistent Image
Are you sure you want to restore the volumes from this persistent image?
Name: snapshots\snapshot.1
Volumes: C:
Date and time: 4/16/2003 4:42:23 PM
Choosing OK will restore the listed volumes from this persistent image.
WARNING:
Restoring this persistent image will revert the volumes indicated to the state that existed when the persistent image was created. Any changes that occurred to these volumes after this date will be lost.
OK
Cancel
Done
Local intranet

Figure 25: Restore confirmation screen

4. After selecting **Restore** the **Are you sure screen** will appear.
5. Choose **OK**.

Note: PSM will not allow the restoration of the system partition from a snapshot. No error is issued, it simply will not revert the volume. PSM protects the system partition against the revert operation, since it would potentially lead the operating system in an inconsistent state.

Known Issues

These were the known issues at time of publication. Please refer to the release notes for the NAS 1000s for updated information regarding known issues.

Event log error at cache full

The eventlog error a driver below this one has failed in some way may occur when the cached file is full.

Display Error on SAK

Status events not rendered properly on SAK. The percent signs not displayed value substitutions missing in displayed message

Always Keep error at cache file full

If all your snapshots on C:\ are tagged as **Always Keep** and the cache file fills up, the system may experience a BSOD at reboot.

It is not recommended to flag all snapshots as **Always Keep** because this disallows the PSM deletion logic to delete the older snapshots to free up cache file space.

Improper display of default Cache File Size

You must delete all snapshots before changing the cache size.

Page file setting

The **Page file size** must not change and the initial size must be set equal to the maximum size. This setting is located in the **Virtual Memory** settings under **System Properties**.

No Boot - No Revert

If the system cannot boot, a revert operation cannot be performed.

Reverting of System Drive Prohibited

PSM does not allow the ability to revert the system boot drive.

No support for mount points in UNIX, AppleTalk, or NetWare

Microsoft confirmed that the Microsoft NFS Services for UNIX, Services for Macintosh, and Services for NetWare do not support volume mount points. These clients will not be able to access data on volumes mounted using a volume mount point. Since snapshots for a volume are mounted as directory junctions (AKA mount points), and even though they are shared these clients will not be able to access the snapshots.

Please refer to the Microsoft Release Notes for Microsoft Server Appliance Kit dated June 2001.

User and Group Management

4

The HP StorageWorks NAS 1000s supports a variety of file sharing protocols for file access over a network, including:

- Common Internet File System (CIFS)
- Network File System (NFS)
- Novell Core Protocol (NCP)
- AppleTalk (AFP)

Access to shares requires a network logon (username and password). It follows that a fundamental part of managing shares involves managing the users and groups that have access.

There are two system environments for users and groups: workgroup and domain. Because users and groups in a domain environment are managed through standard Windows NT or Windows 2000 domain administration methods, this document discusses only local users and groups, which are stored and managed on the NAS device. For information on managing users and groups on a domain, refer to the domain documentation.

The following topics are addressed in this chapter:

- Domain Compared to Workgroup Environments
- User and Group Name Planning
  - Managing User Names
  - Managing Group Names
- Workgroup User and Group Management
  - Managing Local Users
  - Managing Local Groups
- Drive Quotas
  - Managing quotas
  - Enabling and disabling quota management
  - Creating new quota entries for a user or group
  - Deleting new quota entries for a user or group
  - Modifying new quota entries for a user or group

Domain Compared to Workgroup Environments

NAS 1000s devices can be deployed in workgroup or domain environments. When in a domain environment, the server is a member of the domain. The domain controller is a repository of accounts and account access for the NAS 1000s. Client machines are also members of the domain, and users log on to the domain through their Windows clients. The domain controller also administers user accounts and appropriate access levels to resources that are a part of the domain.

In a CIFS environment, when mapping a network drive or a client machine, a user sends a logon credential to the server. This credential includes the username, password, and if appropriate, domain information. Using the credential, the server authenticates and provides the corresponding access to the user.

When a NAS 1000s is deployed into a workgroup environment, all user and group account access permissions to file resources are stored locally on the server.

By contrast, when a NAS 1000s is deployed into a domain environment it uses the account database from the domain controller, with user and group accounts stored outside the server. The server integrates with the domain controller infrastructure.

Note: The NAS 1000s cannot act as a domain controller for other servers on the network. If user and group account information is stored locally, those accounts may be used only to authenticate logons to the NAS 1000s, resulting in a workgroup configuration.

Administering users and groups in a domain environment is similar in a mechanical sense to administering them in a workgroup environment. If using an Active Directory domain controller, the Computer Management tool allows for adding, modifying, and removing users in the same context as in a workgroup environment. The concepts, however, are very different.

Additional information about planning for domain environments can be found at:

http://www.microsoft.com/windows2000/technologies/directory/ad/default.asp

The configuration of the domain controller is reflected on the NAS 1000s because it obtains user account information from the domain controller when deployed in a domain environment. As mentioned previously, the server cannot act as a domain controller itself.

User and Group Name Planning

Effective user and group management is dependent upon how well the user and group names are organized. Administrators typically create a small number of groups on the network and then assign users to the appropriate group or groups. File system and share permissions can then be applied at the group level, rather than at the user level. If the number of groups is small, assigning the appropriate permissions to selected group, or groups, is more efficient than assigning permissions to each user.

Although each organization has specific conventions, following general guidelines makes administration simpler and more efficient. Because CIFS is dependent on users and groups to grant appropriate access levels to file shares, CIFS administration benefits from a consistent user and group administration strategy.

Managing User Names

Usernames should reflect a logical relationship between the username and the person who uses the account. It is important that rules are established to ensure that usernames are:

- Systematic
- Easy to follow and implement
- Easy to remember

Using a combination of the user's first name, middle initial, and last name results in systematic usernames for every member of a particular organization. Common examples include:

- First initial followed by last name (jdoe for John Doe)
- First initial followed by middle initial and last name (jqpublic for John Q. Public)
- First name followed by last name, separated by a period (john.smith for John Smith)
- Last name followed by first initial (doej for Jane Doe)

Guidelines must be in place for instances when two users have the same initials or name. For example, a number can be added to the end of the username (jdoe1 and jdoe2).

Other conventions can be applied. Just ensure that conventions are both systematic and consistent.

Managing Group Names

Group management follows many of the same principles as user management.

It is recommended that group naming conventions be systematic and easy to understand. Make the group name convey some logical information about the function or purpose of the group. Table 3 provides examples of group names.

Table 3: Group Name Examples

Group Name	Description
Administrators	All designated administrators on the server
Users	All standard server users
Power users	All standard server users requiring advanced access levels

Using tags is a helpful convention that indicates the specific access that a particular user has to a network resource. For example, if there is a data share on the device, the network administrator can create a "Data Users ROnly" group and a "Data Users RWrite" group to contain users that have read only or read write access on the share, respectively.

Workgroup User and Group Management

In a workgroup environment, users and groups are managed through the WebUI of the NAS 1000s. Within the Users option, there are two choices:

- Managing local users
- Managing local groups

User and group administrative tasks include adding, deleting, and modifying user and group information. Managing local users and managing local groups are discussed in the following paragraphs.

Managing Local Users

Managing users includes the following tasks:

- Adding a new user
- Deleting a user
- Setting a user password
- Modifying user properties

In the WebUI, under **Users**, **Local Users** is the **Local Users on Server Appliance** dialog box. All workgroup user administration tasks are performed in the **Local Users** dialog box.

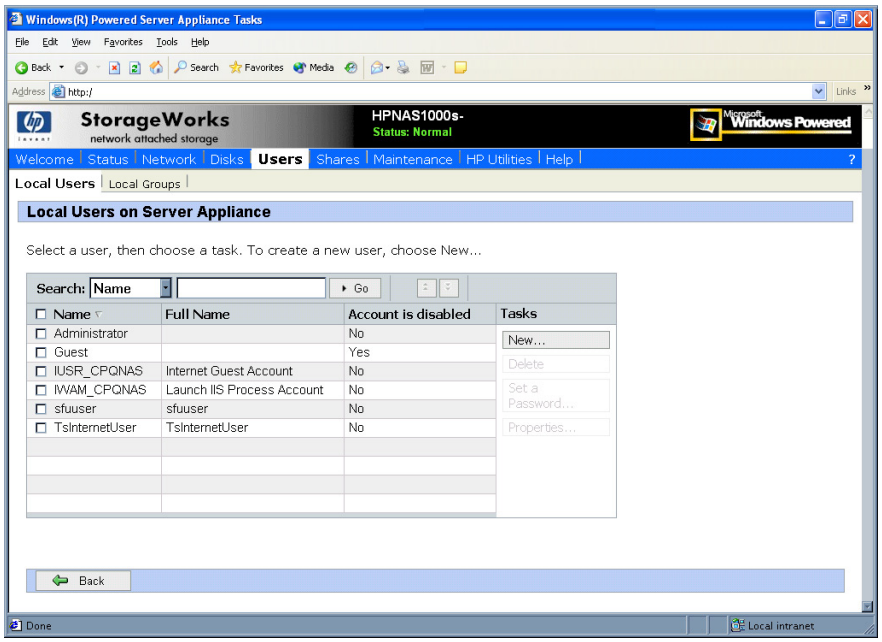

Figure 26: Local Users dialog box

All available options include: **New**, **Delete**, **Set a Password**, and **Properties**. When the **Local Users** dialog box is initially displayed, only the **New** option is available. After an existing user is selected, the additional actions are displayed. Each of these options is discussed in the following paragraphs.

Existing user records can be retrieved in one of two ways:

- By entering the user's User Name or Full Name in the Search fields to retrieve a specific user record. To redisplay the complete user list, space out the Search field.
- By selecting the user from the list of displayed users in the dialog box. The sort order of the display is controlled by clicking the Name field heading. The names are displayed in alphanumeric order or reverse alphanumeric order.

Adding a New User

To add a user:

1. From the **Local Users** dialog box, click **New**. The **Create New User** dialog box is displayed.

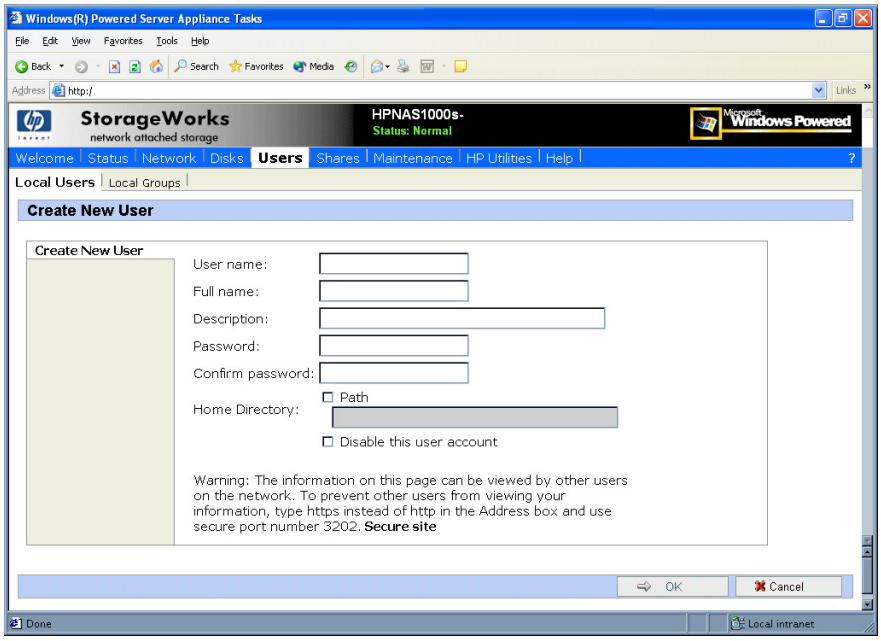
Windows(R) Powered Server Appliance Tasks
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http:/
Links
StorageWorks
network attached storage
HPNAS1000s-
Status: Normal
Microsoft Windows Powered
Welcome Status Network Disks Users Shares Maintenance HP Utilities Help
Local Users Local Groups
Create New User
Create New User
User name:
Full name:
Description:
Password:
Confirm password:
Path
Home Directory:
Disable this user account
Warning: The information on this page can be viewed by other users on the network. To prevent other users from viewing your information, type https instead of http in the Address box and use secure port number 3202. Secure site
OK
Cancel
Done
Local intranet

Figure 27: Create New User dialog box

2. Enter the user information and then click **OK**. The user is added and the **Local Users** dialog box is displayed again.

Deleting a User

To delete a user:

1. In the **Local Users** dialog box, select the user to delete, and then click **Delete**.

   The **Delete User** dialog box is displayed, including a warning note about deleting users.

2. To delete the user, click **OK**. The user is deleted and the **Local Users** dialog box is displayed again.

Modifying a User Password

Follow these steps to modify a user password:

1. In the **Local Users** dialog box, select the user whose password needs to be changed. Then, click **Set a Password**.

   The **Set Password** dialog box is displayed.

2. Enter the password and click **OK**. The Local Users dialog box is displayed again.

Modifying User Properties

To modify other user properties:

1. From the **Local Users** dialog box, select the user whose record needs to be modified. Then, click **Properties**.

   The General information page of the **Properties** dialog box is displayed. Figure 28 is an illustration of the **User Properties** dialog box.

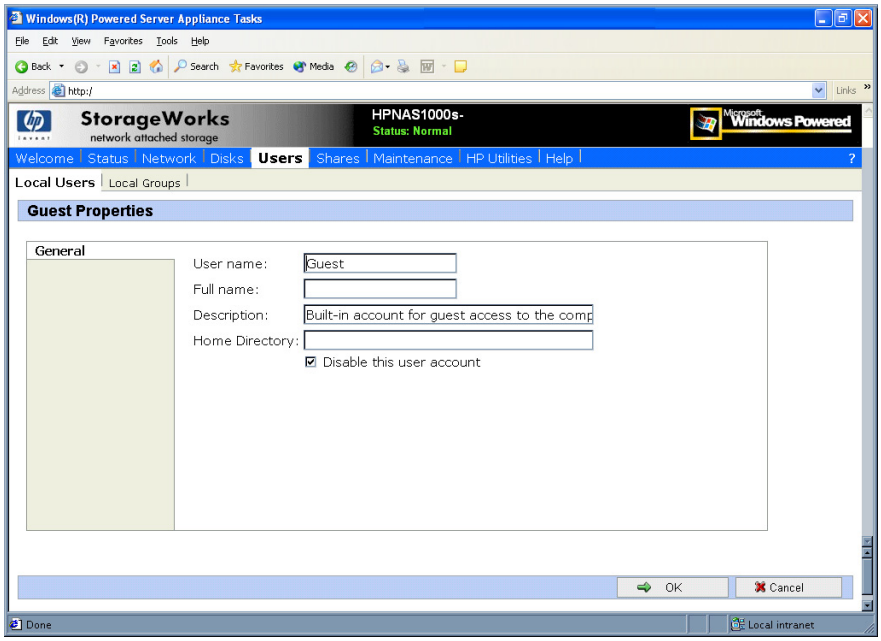

Figure 28: User Properties dialog box

2. The following information can be changed or set:
   - User name
   - Full name
   - Description
   - Home Directory
   - Disable this user account
3. After completing the changes, click **OK**. The **Local Users** dialog box is displayed again.

Managing Local Groups

Managing groups includes the following tasks:

- Adding a new group
- Deleting a group
- Modifying group properties, including user memberships

Local groups in a workgroup environment are managed through the Users option in the WebUI.

In the WebUI, under **Users**, **Local Groups** is the **Local Groups on Server Appliance** dialog box. All workgroup group administration tasks are performed in the **Local Groups on Server Appliance** dialog box.

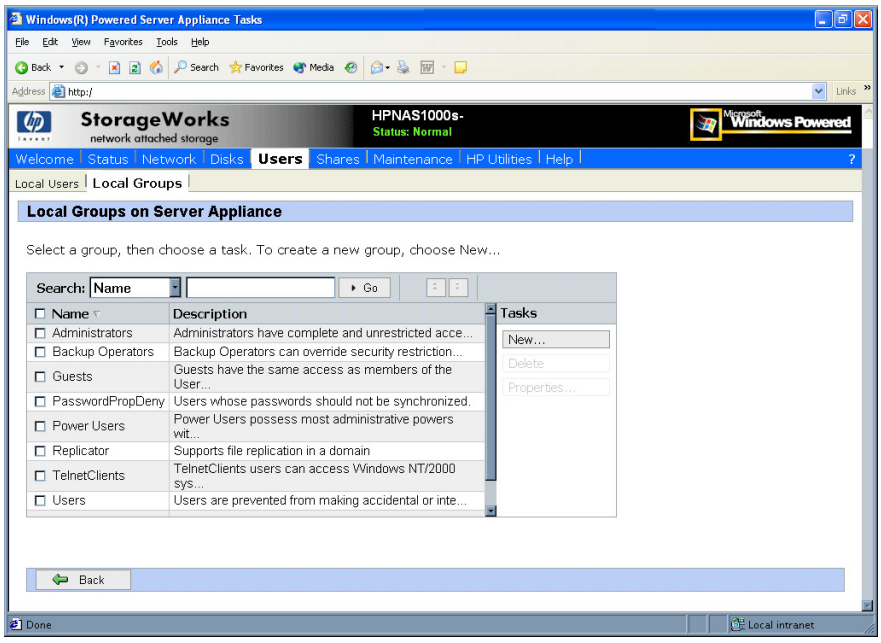
Windows(R) Powered Server Appliance Tasks
File Edit View Favorites Tools Help
StorageWorks
network attached storage
HPNAS1000s-
Status: Normal
Windows Powered
Welcome Status Network Disks Users Shares Maintenance HP Utilities Help
Local Users Local Groups
Local Groups on Server Appliance
Select a group, then choose a task. To create a new group, choose New...
Search: Name Go
Name Description
Administrators Administrators have complete and unrestricted acce...
Backup Operators Backup Operators can override security restriction...
Guests Guests have the same access as members of the User...
PasswordPropDeny Users whose passwords should not be synchronized.
Power Users Power Users possess most administrative powers wit...
Replicator Supports file replication in a domain
TelnetClients TelnetClients users can access Windows NT/2000 sys...
Users Users are prevented from making accidental or inte...
Tasks
New...
Delete
Properties...
Back
Done
Local intranet

Figure 29: Local Groups dialog box

Adding a New Group

To add a group:

1. In the **Local Groups** dialog box, click **New**.

   The **Create New Group** dialog box is displayed.

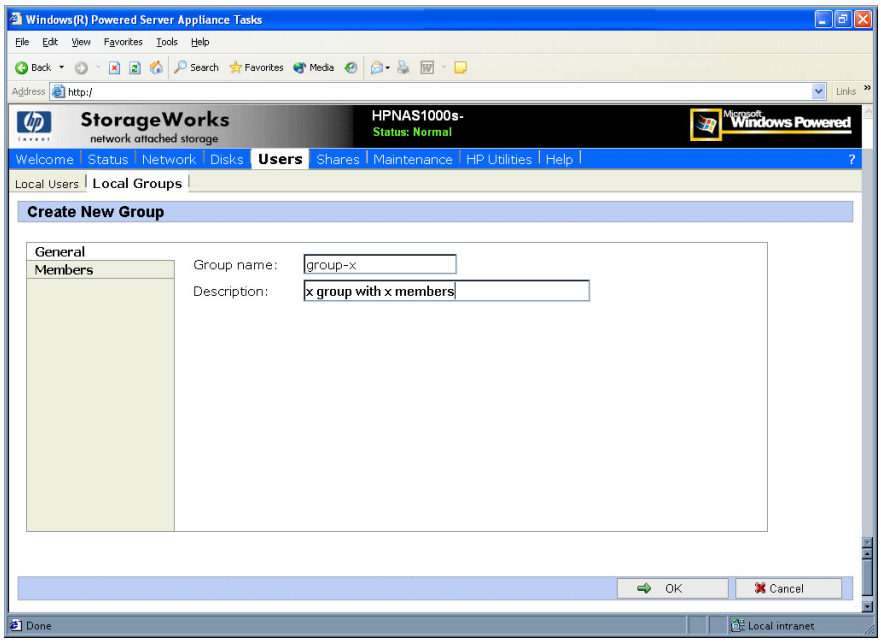

Figure 30: Create New Group dialog box, General tab

2. Enter the group name and description.
3. To indicate the user members of this group, click **Members**. See "Modifying Group Properties" for procedural instructions on entering group members.
4. After all group information is entered, click **OK**. The group is added, and the **Local Groups** dialog box is displayed again.

Deleting a Group

To delete a group:

1. From the **Local Groups** dialog box, select the group to delete, and then click **Delete**.
2. The **Delete Group** dialog box is displayed. Verify that this is the intended group and then click **OK**. The **Local Groups** dialog box is displayed again.

Modifying Group Properties

To modify other group properties:

1. From the **Local Groups** dialog box, select the desired group and then click **Properties**. The **Properties** dialog box is displayed.

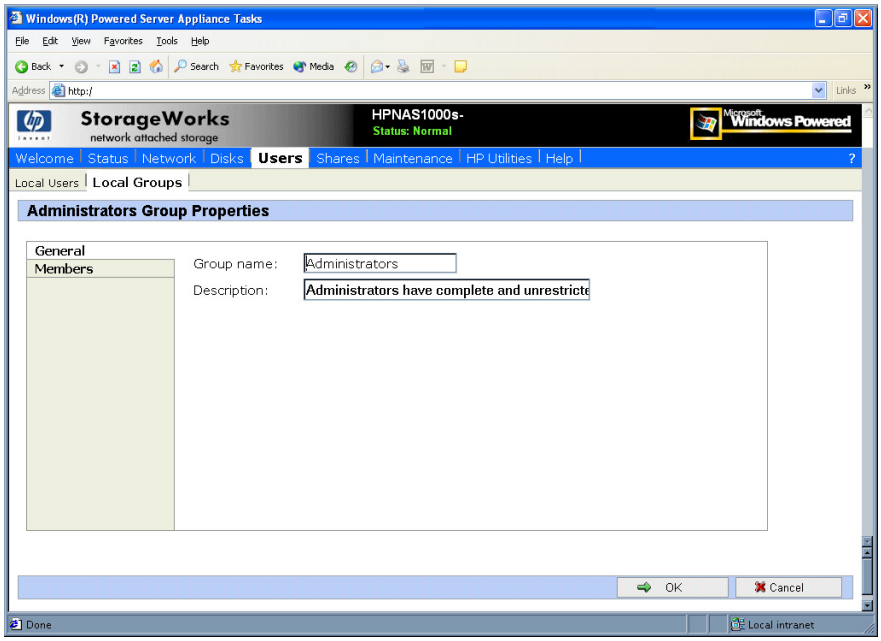

Figure 31: Group Properties dialog box, General tab

Within the Properties dialog box are two tabs:

- General tab
- Members tab

Each of these tabs is discussed in the following paragraphs.

2. Enter the desired changes in each of the tabs. Then, click **OK**. The **Local Groups** dialog box is displayed again.

General Tab

Within the General tab, basic group information can be changed, including:

- Group name
- Description

Members Tab

To indicate or change the members of a group, click the **Members** tab. Within this dialog box, users are added and removed from a group.

Two boxes are displayed: **Members** and **Add user or group**. Current members of that group are listed in the **Members** box. All users are listed in the **Add user or group** box.

- *To add an existing local user to a group*, select the desired user from the **Add user or group** box and then click the **Add** button.

- *To remove an existing local user from a group*, select the desired user from the **Members** box, and then click the **Remove** button.
- *To add user or group from a domain to this group*, the scroll bar at the right of the screen may need to be used to scroll up the screen display. Enter the user or group name to include in the indicated format (domain/user).

Figure 32 is an example of the **Members** tab.

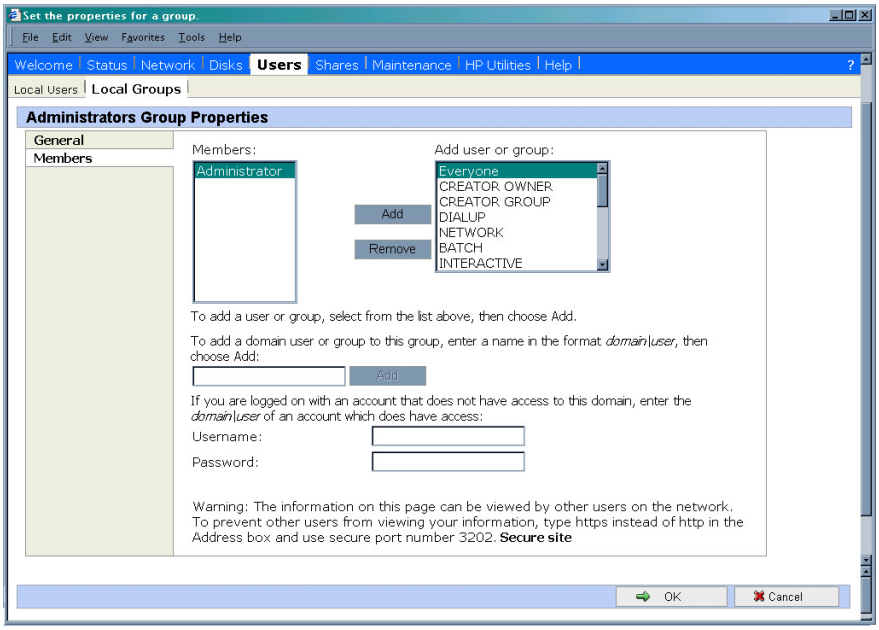
Set the properties for a group.
File Edit View Favorites Tools Help
Welcome Status Network Disks Users Shares Maintenance HP Utilities Help
Local Users Local Groups
Administrators Group Properties
General
Members
Members:
Administrator
Add user or group:
Everyone
CREATOR OWNER
CREATOR GROUP
DIALUP
NETWORK
BATCH
INTERACTIVE
Add
Remove
To add a user or group, select from the list above, then choose Add.
To add a domain user or group to this group, enter a name in the format domain\user, then choose Add:
Add
If you are logged on with an account that does not have access to this domain, enter the domain\user of an account which does have access:
Username:
Password:
Warning: The information on this page can be viewed by other users on the network. To prevent other users from viewing your information, type https instead of http in the Address box and use secure port number 3202. Secure site
OK
Cancel

Figure 32: Group Properties dialog box, Members tab

Drive Quotas

Drive quotas let administrators control the allocation of drive space to individual users or groups of users. When quotas are enabled and properly configured, it is impossible for one person or group to consume all of the available space on a disk.

When quotas are enabled on a volume that already contains files, the system calculates the drive space used by all users on the volume. The quota limit and warning level are then applied to all current users. Administrators can then modify quotas as needed. By enabling and then disabling quotas, administrators take advantage of the auditing capabilities provided by quotas, without reducing server performance.

Managing Quotas

Managing quotas includes:

- Enabling and disabling quota management
- Creating new quota entries for a user or group
- Deleting quota entries for a user or group
- Modifying quota entries for a user or group

Each of these tasks is discussed in the following sections.

Quota management tasks are performed from the **Disks**, **Disk Quota** selection from the WebUI menu. Figure 33 is an illustration of the disk quota dialog box.

Note: If the volume is not formatted with the NTFS file system, or if you are not a member of the administrators group, the Disk Quota option is not displayed (not accessible).

Note: For more information about quotas, refer to online help for NAS device quota help.

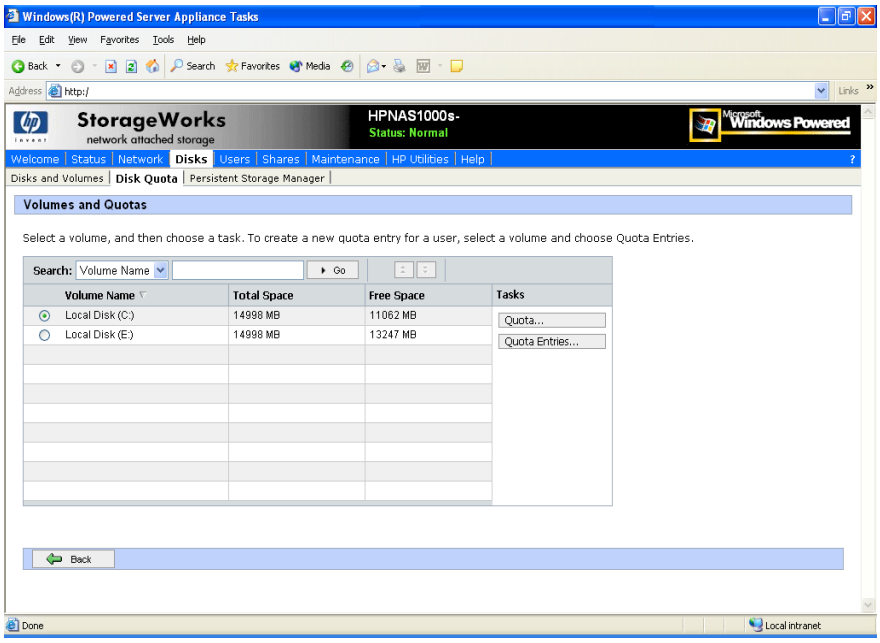
Windows(R) Powered Server Appliance Tasks
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http:/
Links
StorageWorks
network attached storage
HPNAS1000s-
Status: Normal
Microsoft Windows Powered
Welcome Status Network Disks Users Shares Maintenance HP Utilities Help
Disks and Volumes Disk Quota Persistent Storage Manager
Volumes and Quotas
Select a volume, and then choose a task. To create a new quota entry for a user, select a volume and choose Quota Entries.
Search: Volume Name Go
Volume Name Total Space Free Space Tasks
Local Disk (C:) 14998 MB 11062 MB
Local Disk (E:) 14998 MB 13247 MB
Quota...
Quota Entries...
Back
Done
Local intranet

Figure 33: Disk Quota dialog box

Enabling and Disabling Quota Management

To enable drive quotas:

1. From the WebUI, select **Disks**, **Disk Quota**. From the **Volumes and Quotas** dialog box, select a volume, and then click **Quota**. The **Default Quota** dialog box for the specified volume is displayed.

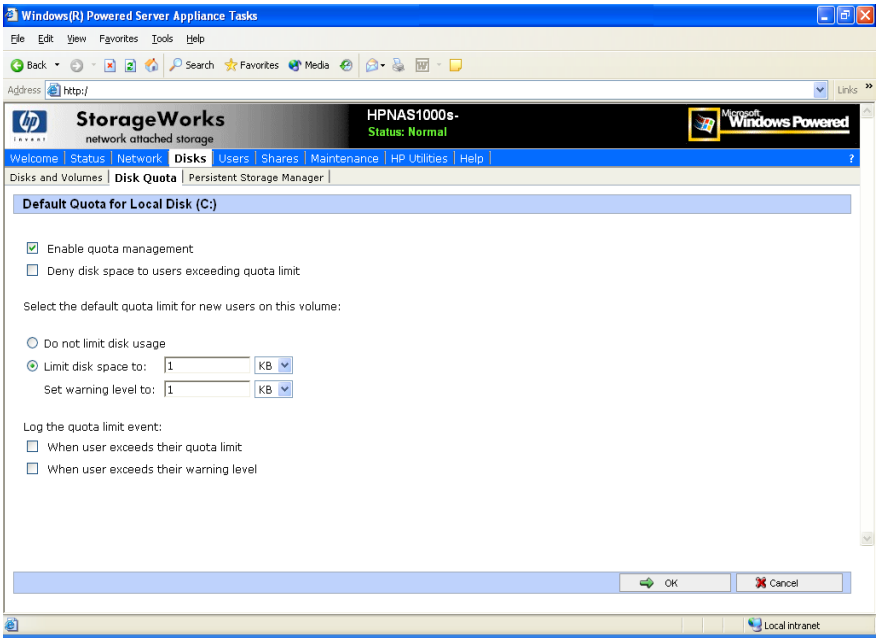
Windows(R) Powered Server Appliance Tasks
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http:/
Links
StorageWorks
network attached storage
HPNAS1000s-
Status: Normal
Microsoft Windows Powered
Welcome Status Network Disks Users Shares Maintenance HP Utilities Help
Disks and Volumes Disk Quota Persistent Storage Manager
Default Quota for Local Disk (C:)
Enable quota management
Deny disk space to users exceeding quota limit
Select the default quota limit for new users on this volume:
Do not limit disk usage
Limit disk space to: 1 KB
Set warning level to: 1 KB
Log the quota limit event:
When user exceeds their quota limit
When user exceeds their warning level
OK
Cancel
Local intranet

Figure 34: Default Quota dialog box

2. To enable quotas on the selected disk, select **Enable quota management**. Compete the additional data fields on the screen, including disk space and warning level limits and auditing settings.
3. To disable quotas on the selected disk, de-select **Enable quota management**.
4. After completed all field entries, click **OK**. The **Volume and Quotas** dialog box is displayed again.

Creating New Quota Entries for a User or Group

To create new quotas for a user or group:

1. From the WebUI, select **Disks**, **Disk Quotas**. In the **Volumes and Quotas** dialog box, select a volume and then click **Quota Entries**. The **Quota Entries** dialog box is displayed.

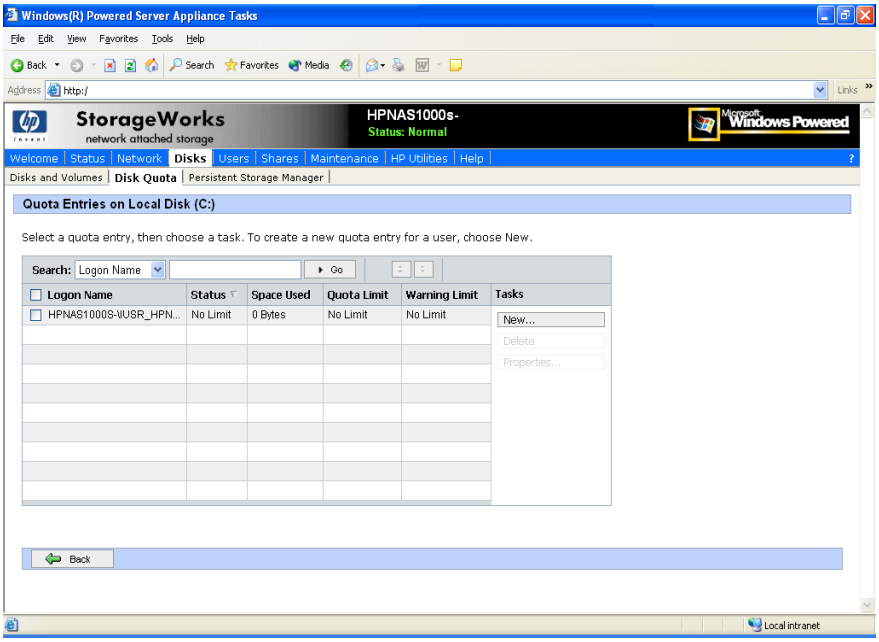
Windows(R) Powered Server Appliance Tasks
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http:/
Links
StorageWorks
network attached storage
HPNAS1000s-
Status: Normal
Microsoft Windows Powered
Welcome Status Network Disks Users Shares Maintenance HP Utilities Help
Disks and Volumes Disk Quota Persistent Storage Manager
Quota Entries on Local Disk (C:)
Select a quota entry, then choose a task. To create a new quota entry for a user, choose New.
Search: Logon Name Go
Logon Name Status Space Used Quota Limit Warning Limit Tasks
HPNAS1000S-\IUSR_HPN... No Limit 0 Bytes No Limit No Limit
New...
Delete
Properties...
Back
Local intranet

Figure 35: Quota Entries dialog box

2. All users and groups with established quotas are displayed. To create a new quota for a user or group, click **New**. The **New Quota Entry** dialog box is displayed.

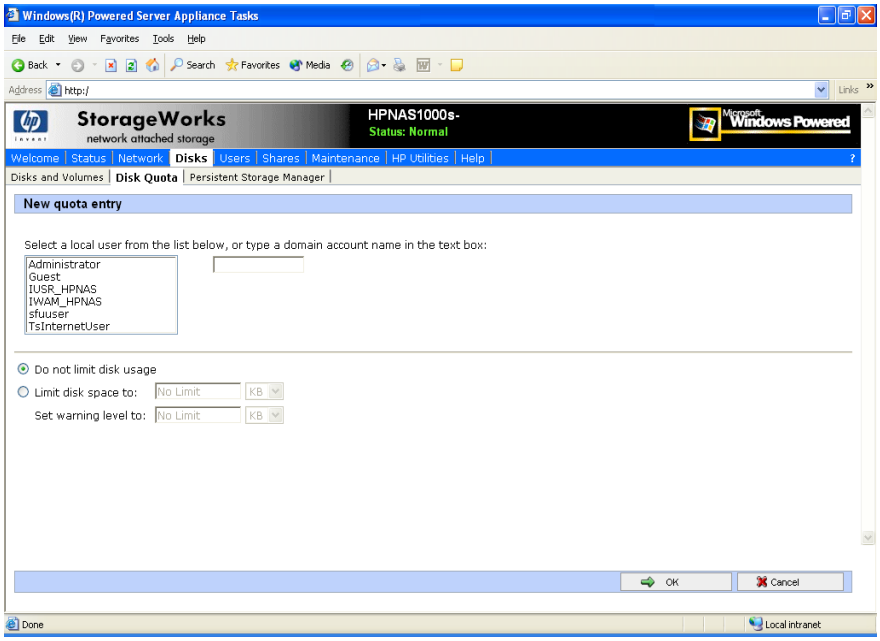

Figure 36: New Quota Entry dialog box

3. Indicate the user that the quota is for. For local users and groups, select the desired user from the **Select a local user** box. For users on the domain, enter the user's domain account name in the indicated box.
4. Enter a disk space limit.
5. Verify the accuracy of the field entries, and then click **OK**. The **Quota Entries** dialog box is displayed again.

Deleting Quota Entries for a User or Group

To delete quotas for a user or group:

1. From the WebUI, select **Disks**, **Disk Quotas**. In the **Volumes and Quotas** dialog box, select a volume and then click **Quota Entries**. The **Quota Entries** dialog box is displayed.
2. All users and groups with established quotas are displayed. To delete a quota for a user or group, click **Delete**. A verification dialog box is displayed.
3. Verify that this is the correct user, and then click **OK**. The **Quota Entries** dialog box is displayed again.

Modifying Quota Entries for a User or Group

Usage limit parameters for a user's quota can be changed. To modify these user quota settings:

1. From the WebUI, select **Disks**, **Disk Quotas**. In the **Volumes and Quotas** dialog box, select a volume and then click **Quota Entries**. The **Quota Entries** dialog box is displayed.
2. All users and groups with established quotas are displayed. To modify quota for a user or group, select a user, and then click **Properties**. The **Quota Entry** dialog box for that user is displayed.

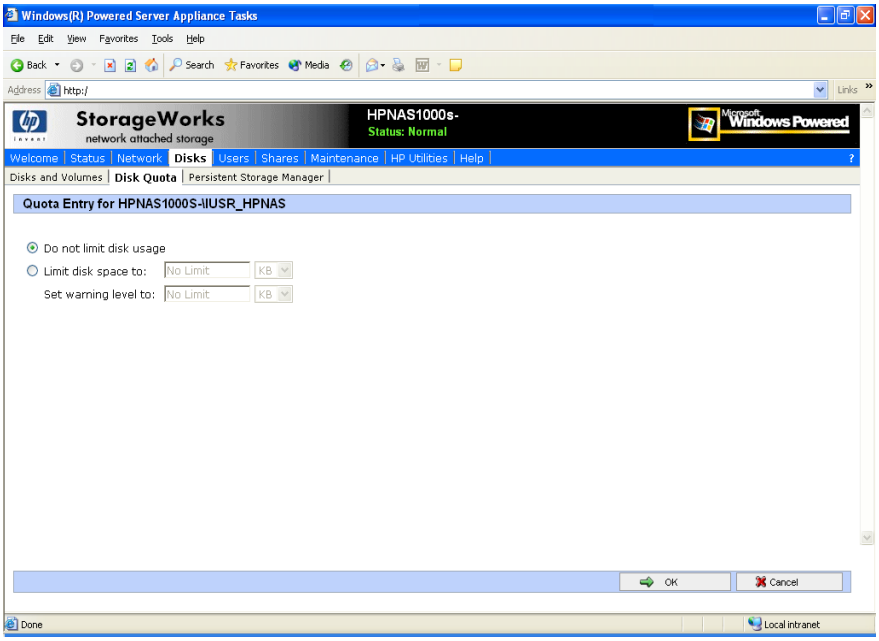

Figure 37: Quota Entry dialog box for a user

3. Enter the new disk limit information, and then click **OK**. The **Quota Entries** dialog box is displayed again.

Folder and Share Management

5

The HP StorageWorks NAS 1000s supports several file sharing protocols, including CIFS, NFS, FTP, HTTP, NCP, and AFP (AppleTalk). This chapter discusses overview information as well as procedural instructions for the setup and management of the file shares for the supported protocols. In addition, discussions on security at the file level and at the share level are included in this chapter.

Abbreviated information on creating NFS file shares is included in this chapter; for detailed information on setting up and managing NFS file shares, see Chapter 6, UNIX File System Management.

NCP shares must be set up and managed through the NAS Management Console user interface. For information on managing NCP file shares, see Chapter 7, NetWare File System Management.

More information about Windows file system security is available on the Microsoft website:

www.microsoft.com/

The following topics are discussed in this chapter:

- Folder Management
  - Navigating to a Specific Volume or Folder
  - Creating a New Folder
  - Deleting a Folder
  - Modifying Folder Properties
  - Creating a New Share for a Volume or Folder
  - Managing Shares for a Volume or Folder
  - Managing File Level Permissions
- Share Management
  - Share Considerations
  - Defining Access Control Lists
  - Integrating Local File System Security into Windows Domain Environments
  - Comparing Administrative (Hidden) and Standard Shares
  - Planning for Compatibility between File Sharing Protocols

- Managing Shares
  - Creating a new share
  - Deleting a share
  - Modifying share properties
  - CIFS sharing
  - NFS sharing
  - FTP sharing
  - Web sharing (HTTP)
  - Netware sharing (NCP)
  - AFP (AppleTalk) sharing
  - Installing services for AppleTalk
  - Installing Windows NT Services for Macintosh
- Protocol Parameter Settings

All procedures in this chapter are documented using the WebUI. In addition to this guide, you may use the WebUI online help.

Folder Management

Volumes and folders on any system are used to organize data. Regardless of system size, systematic structuring and naming conventions of volumes and folders eases the administrative burden. Moving from volumes to folders to shares increases the level of granularity of the types of data stored in the unit and the level of security access allowed.

Although a variety of methods can be used to create and manage file folders on the NAS 1000s, this document discusses using the NAS Web based user interface (WebUI.)

Managing system volumes and file folders includes the following tasks:

- Navigating to a specific volume or folder
- Creating a new folder
- Deleting a folder
- Modifying folder properties
- Creating a new share for a volume or folder
- Managing shares for a volume or folder
- Managing file level permissions

Navigating to a Specific Volume or Folder

When you work with volumes and folders, the first task is to gain access to the desired volume or folder.

The steps are the same, whether navigating to a volume or a folder:

1. To navigate to a specific volume or folder, from the WebUI, select **Shares** and then **Folders**. Initially, the **Volumes** dialog box is displayed.

   This initial dialog box displays all system volumes.

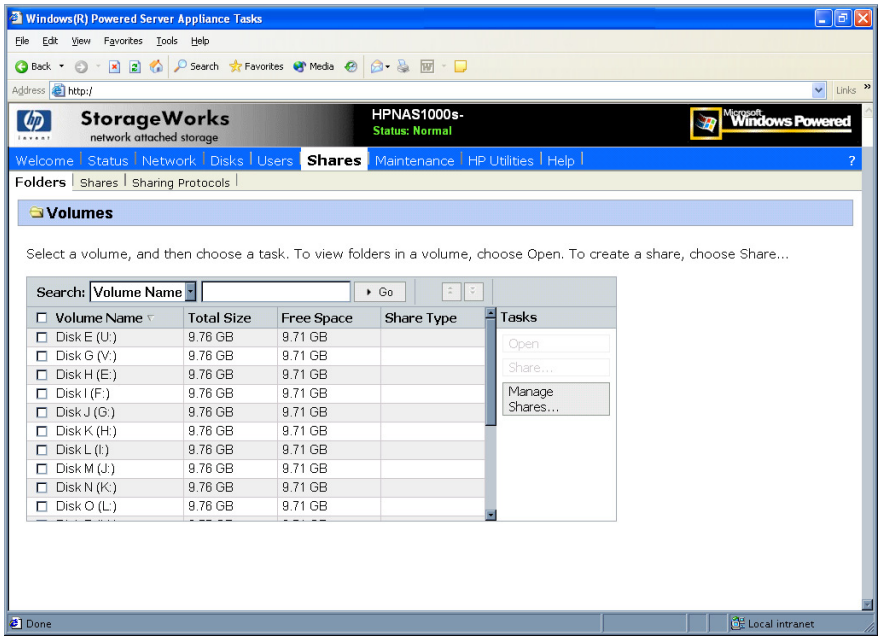
Windows(R) Powered Server Appliance Tasks
File Edit View Favorites Tools Help
StorageWorks
network attached storage
HPNAS1000s-
Status: Normal
Windows Powered
Welcome Status Network Disks Users Shares Maintenance HP Utilities Help
Folders Shares Sharing Protocols
Volumes
Select a volume, and then choose a task. To view folders in a volume, choose Open. To create a share, choose Share...
Search: Volume Name Go
Volume Name Total Size Free Space Share Type
Disk E (U:) 9.76 GB 9.71 GB
Disk G (V:) 9.76 GB 9.71 GB
Disk H (E:) 9.76 GB 9.71 GB
Disk I (F:) 9.76 GB 9.71 GB
Disk J (G:) 9.76 GB 9.71 GB
Disk K (H:) 9.76 GB 9.71 GB
Disk L (I:) 9.76 GB 9.71 GB
Disk M (J:) 9.76 GB 9.71 GB
Disk N (K:) 9.76 GB 9.71 GB
Disk O (L:) 9.76 GB 9.71 GB
Tasks
Open
Share...
Manage Shares...
Done
Local intranet

Figure 38: Volumes dialog box

2. From this dialog box, navigate to a specific folder by selecting the appropriate volume and then clicking **Open**. The **Folders** dialog box is displayed, with a list of all of the folders within that volume.
3. To navigate to a subfolder, select the folder in which the subfolder resides, and then click **Open**. Repeat this searching and opening process until the desired folder is opened. See Figure 39 for an example of **Folders** dialog box.

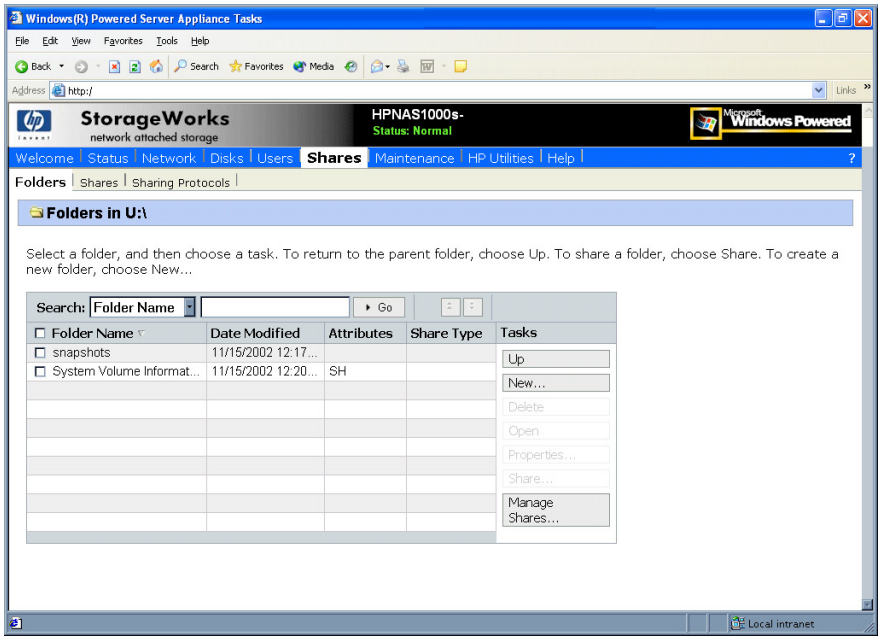
Windows(R) Powered Server Appliance Tasks
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http:/
Links
StorageWorks
network attached storage
HPNAS1000s-
Status: Normal
Microsoft Windows Powered
Welcome Status Network Disks Users Shares Maintenance HP Utilities Help ?
Folders Shares Sharing Protocols
Folders in U:\
Select a folder, and then choose a task. To return to the parent folder, choose Up. To share a folder, choose Share. To create a new folder, choose New...
Search: Folder Name Go
Folder Name Date Modified Attributes Share Type Tasks
snapshots 11/15/2002 12:17...
System Volume Informat... 11/15/2002 12:20... SH
Up
New...
Delete
Open
Properties...
Share...
Manage Shares...
Local intranet

Figure 39: Folders dialog box

After accessing the desired folder, the following actions can be performed:

- Creating a new folder
- Deleting a folder
- Modifying folder properties
- Creating a new share for the volume or folder
- Managing shares for the volume or folder

Creating a New Folder

To create a new folder:

1. From the **Shares** directory, navigate to the **Folders** menu and then select **New**. The **Create New Folder** dialog box is displayed.

   Two tabs are displayed: **General** and **Compress**. Use these two tabs to enter the parameters for the new folder.

2. In the General tab, enter a name for the folder and specify the folder attributes.

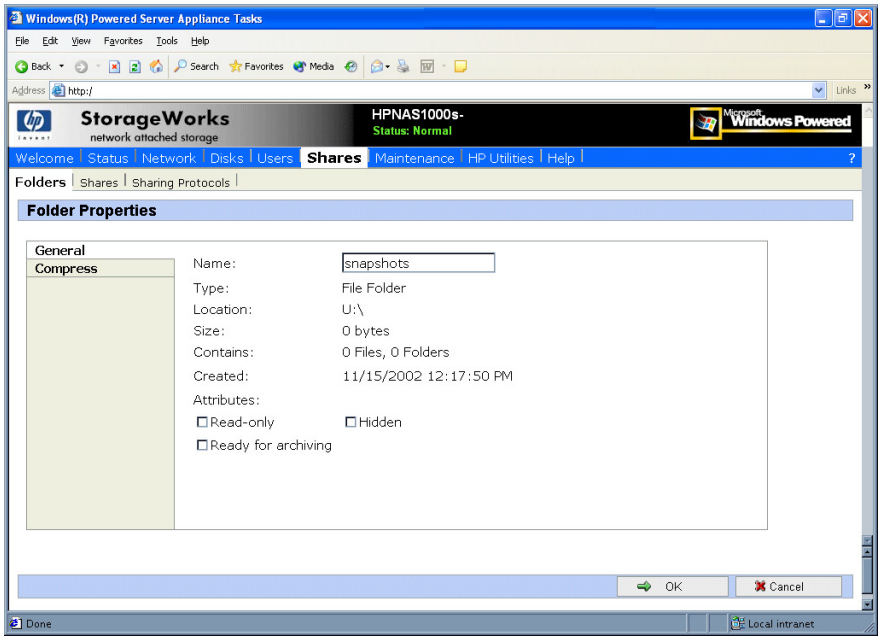

Figure 40: Create a New Folder dialog box, General tab

3. In the **Compress** tab, indicate whether and how this folder and its contents are to be compressed.
4. After all information for the new folder is entered, click **OK**.

Deleting a Folder

To delete a folder:

1. From the **Shares** directory, navigate to the folder to delete. Select the folder and then click **Delete**. The **Delete Folder** dialog box is displayed.

   Summary information about the deletion is displayed.

Note: View the summary information to confirm that this is the intended share.

---

2. Verify that the displayed folder is the folder to delete and then click **OK**.

   The folder and all of its subfolders are deleted and the main dialog box is displayed again.

Modifying Folder Properties

To modify folder properties:

1. From the **Shares** directory, navigate to the folder whose properties need to be edited. Then click **Properties**. The **Properties** dialog box is displayed.

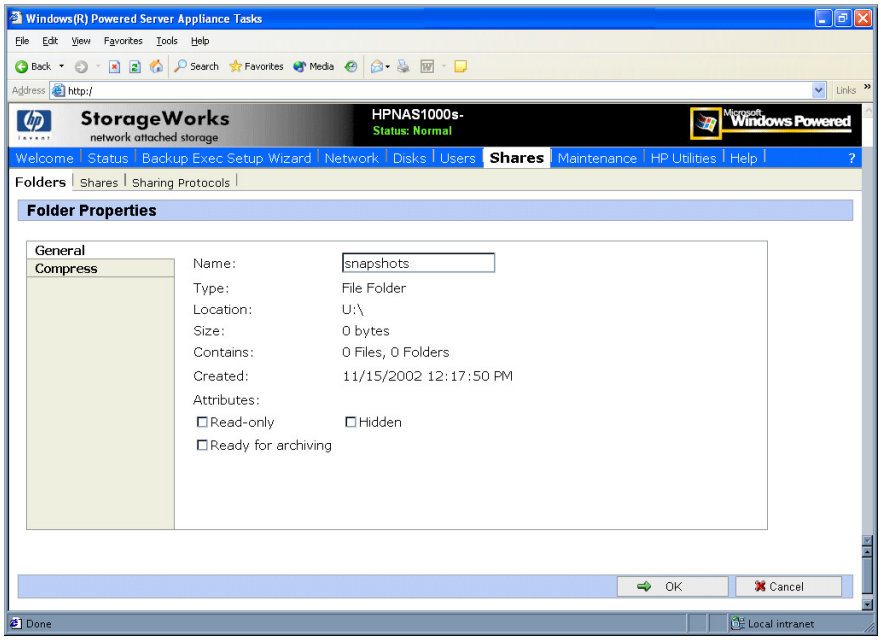

Figure 41: Folder Properties dialog box, General tab

2. In the **General** tab, enter the new information for the folder, which may include:
   - Folder Name
   - Folder Attributes
3. In the **Compress** tab, indicate whether and how this folder and its contents are to be compressed.
4. After all changes have been completed, click **OK**. The **Folders** dialog box is displayed again.

Creating a New Share for a Volume or Folder

Within the WebUI, there are two access points to the same screens used to create file shares:

- A share can be created for a folder while working with that folder in the **Folders** screens.
- A share can be created and, if necessary, new folders can be created, while working with file shares in the **Shares** screens.

This section discusses creating shares from the **Folders** menu, and is an overview of the procedures. Complete details on the process of creating shares are included in the discussion that documents creating shares through the **Shares** menu. See the "Managing Shares" section of this chapter for these details.

To create a new share for a specific volume or folder while in the **Folders** menu:

1. Navigate to the desired volume or folder and click **Share**. The **Create New Share** dialog box is displayed.

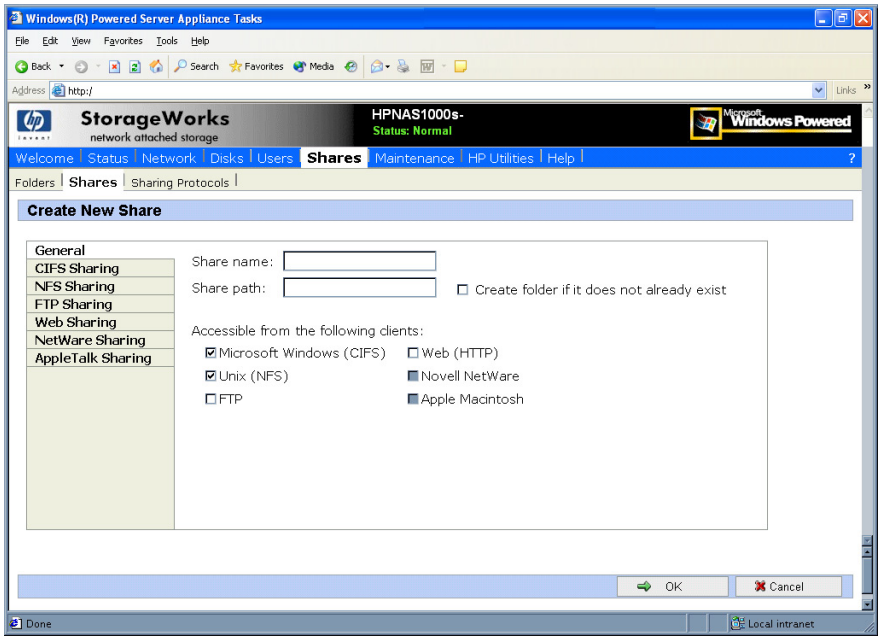

Figure 42: Create New Share dialog box, General tab

2. Enter the information for the share, including the name of the share, the allowed protocols, and corresponding permissions.

Note: The **Share path** is the path of the previously selected volume or folder. This field is automatically completed by the system.

---

3. Select the appropriate tab to enter protocol specific information.

   See the "Managing Shares"section for detailed information about these entries.

4. After entering all share information, click **OK**.

Managing Shares for a Volume or Folder

Within the WebUI, there are two access points to the same screens used to manage file shares:

- While working with a folder in the **Folders** dialog boxes, the administrator can create, delete, and modify shares for that folder.
- While working with file shares in the **Shares** dialog boxes, the administrator can create, delete, and modify shares (and if necessary, create new folders).

Note: This section discusses managing shares from the **Folders** menu, and is an overview of the procedures. Complete details on the process of managing shares are included in the discussion that documents creating shares through the **Shares** menu. See the "Managing Shares" section later in this chapter for these details.

To create, delete, and manage shares for a particular volume or folder while in the **Folders** menu:

1. From the **Folders** directory, navigate to the target volume or folder and click **Manage Shares**. The **Shared Folders** dialog box is displayed.

   All associated shares for that folder or volume are listed.

2. To create a new share, click **New**. The **Create a New Share** dialog box is displayed.

   Because the screens are the same whether shares are managed through the **Folders** menu or the **Shares** menu, the procedures are only documented once. See "Creating a New Share" in the "Share Management" section for detailed procedural instructions on creating new file shares.

3. To delete a share, select the share to delete and click **Delete**. The **Delete Share** dialog box is displayed.

   Because the screens are the same whether shares are managed through the **Folders** menu or the **Shares** menu, the procedures are only documented once. See "Deleting a New Share" in the "Share Management" section for detailed procedural instructions on deleting file shares

4. To modify share properties, select the share to modify, and click **Properties**. The **Share Properties** dialog box is displayed.

   Because the screens are the same whether shares are managed through the **Folders** menu or the **Shares** menu, the procedures are only documented once. See "Moifying Share Properties" in the "Share Management" section for detailed procedural instructions on modifying shares.

Managing File Level Permissions

The WebUI of the NAS 1000s provides security at the share level and is discussed later in this chapter. Security at the file level is managed using Windows Explorer available from the desktop of the NAS 1000s. To access the NAS 1000s Console from the WebUI, go to the **Maintenance** menu and select **Terminal Services**.

File level security includes settings for permissions, ownership, and auditing for individual files.

To enter file permissions:

1. Using Windows Explorer, navigate to the folder or file that needs to be changed and then right-click the folder.
2. Select **Properties** and then select the **Security** tab. Figure 43 illustrates the properties available on the **Security** tab.

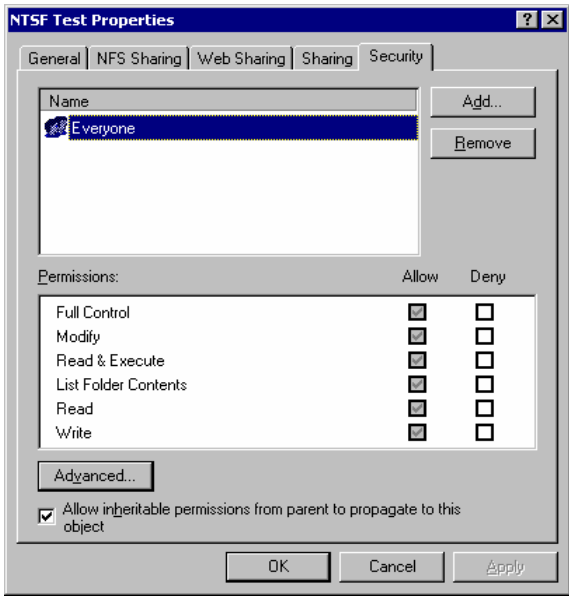

Figure 43: Security Properties dialog box for folder name NTSF Test

Several options are available in the **Security** tab dialog box:

- To add users and groups to the permissions list, click **Add**. Then follow the dialog box instructions.
- To remove users and groups from the permissions list, highlight the desired user or group and then click **Remove**.
- If the **Allow inheritable permissions from parent to propagate to this object** box at the bottom of the screen is checked, the file or directory inherits permissions from the parent directory. In this case, existing user and group permissions cannot be changed; however, additional users or groups can be added.
- The center section of the **Security** tab provides a listing of permission levels. When new users or groups are added to the permissions list, select the appropriate boxes to configure the common file access levels.

Note: Selections can be made when the **Allow inheritable permissions from parent to propagate to this object** box is disabled.

- To modify ownership of files or to modify individual file access level permissions, click **Advanced**.

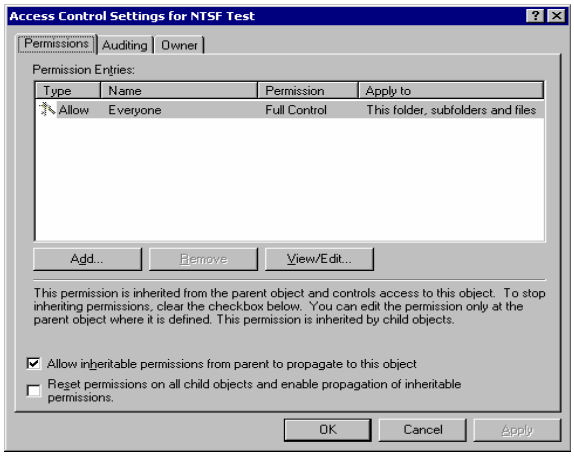
Access Control Settings for NTSF Test
Permissions
Auditing
Owner
Permission Entries:
Type
Name
Permission
Apply to
Allow
Everyone
Full Control
This folder, subfolders and files
Add...
Remove
View/Edit...
This permission is inherited from the parent object and controls access to this object. To stop inheriting permissions, clear the checkbox below. You can edit the permission only at the parent object where it is defined. This permission is inherited by child objects.
Allow inheritable permissions from parent to propagate to this object
Reset permissions on all child objects and enable propagation of inheritable permissions.
OK
Cancel
Apply

Figure 44: Access Control Settings dialog box for folder name NTSF Test, Permissions tab

To modify specific permissions assigned to a particular user or group for a selected file or folder in the **Advanced** screen:

1. Select the desired user or group.
2. Click **View/Edit**.
3. Check all the permissions that you want to enable, and clear the permissions that you want to disable. Enable or disable permissions by selecting the **Allow** box to enable permission or the **Deny** box to disable permission. If neither box is selected, permission is automatically disabled. Figure 45 illustrates the **View/Edit** screen and some of the permissions.

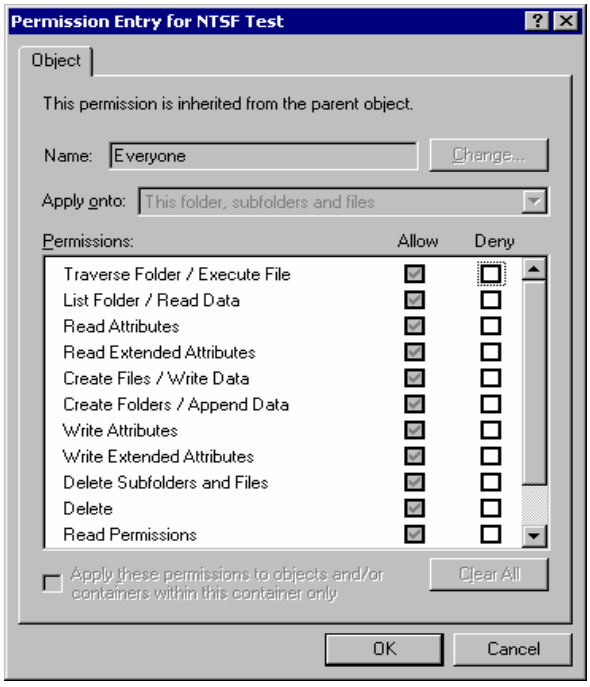

Figure 45: User or Group Permission Entry dialog box for folder name NTSF Test

Other functionality available in the **Advanced Access Control Permissions** tab is illustrated in Figure 45 and includes:

- **Add a new user or group**. Click **Add**, and then follow the dialog box instructions.
- **Remove a user or group**. Click **Remove**.
- **Inherit permissions from the parent folder**. Enable the **Allow inheritable permissions from parent to propagate to this object** box.
- **Reset permissions**. If the object being configured is a folder, check the **Reset permissions on all child objects and enable propagation of inheritable permissions** box, which allows all child folders and files to inherit the current folder permissions by default.

Another area of the **Advanced Access Control** is the **Auditing** tab. Auditing allows you to set rules for the auditing of access, or attempted access, to files or folders. Users or groups can be added, deleted, viewed, or modified through the advanced **Access Control Settings Auditing** tab. The **Auditing** tab dialog box is illustrated in Figure 46.

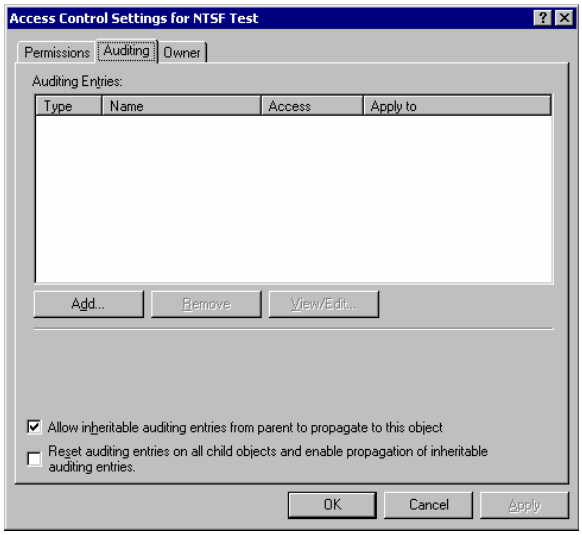

Figure 46: Access Control Settings, Auditing tab dialog box for folder name NTSF Test

Figure 47 illustrates the screen that is displayed when a user or group to be audited is added.

4. Select the appropriate domain or machine name from the **Look in:** drop-down list box at the top of the screen.

Note: A list of users and groups from the desired domain can be viewed if the current user has permission to view the information on the domain.

---

5. Select the user or group.

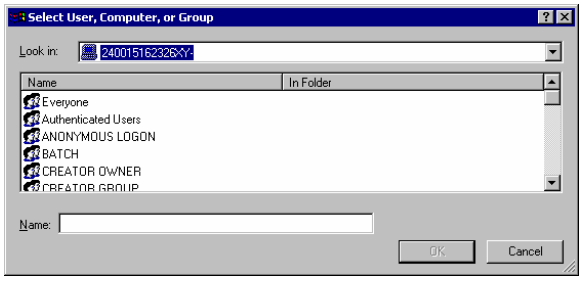

Figure 47: Select User, Computer, or Group dialog box

6. Click **OK**. Figure 48 illustrates the **Auditing Entry** screen that is displayed.

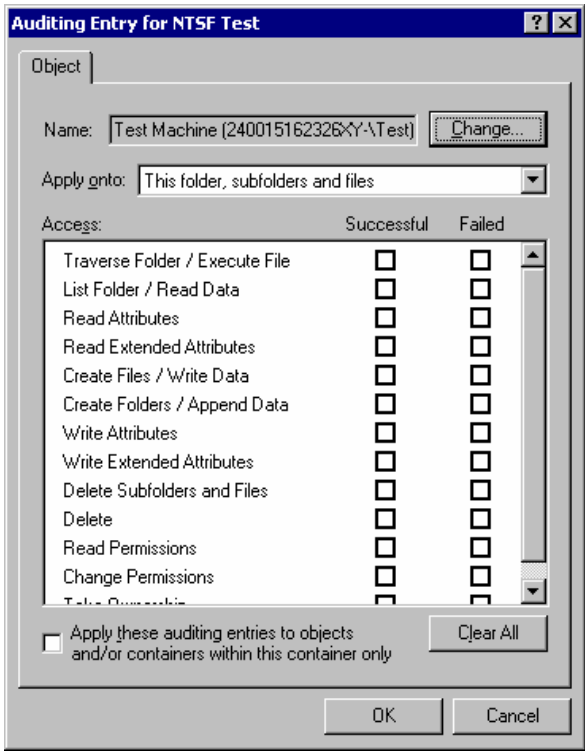

Figure 48: Auditing Entry dialog box for folder name NTSF Test

7. Select the desired **Successful** and **Failed** audits for the user or group as shown in Figure 48.
8. Click **OK**.

Note: Auditing must be enabled to configure this information. Use the local Computer Policy Editor to configure the audit policy on the NAS 1000s.

The final tab in the advanced **Advanced Access Control Settings** security configuration is the **Owner** tab. This tab allows for taking ownership of files. Typically, administrators use this area to take ownership of files when the file ACL is incomplete or corrupt. By taking ownership, you gain access to the files and then manually apply the appropriate security configurations. Figure 49 illustrates the **Owner** tab.

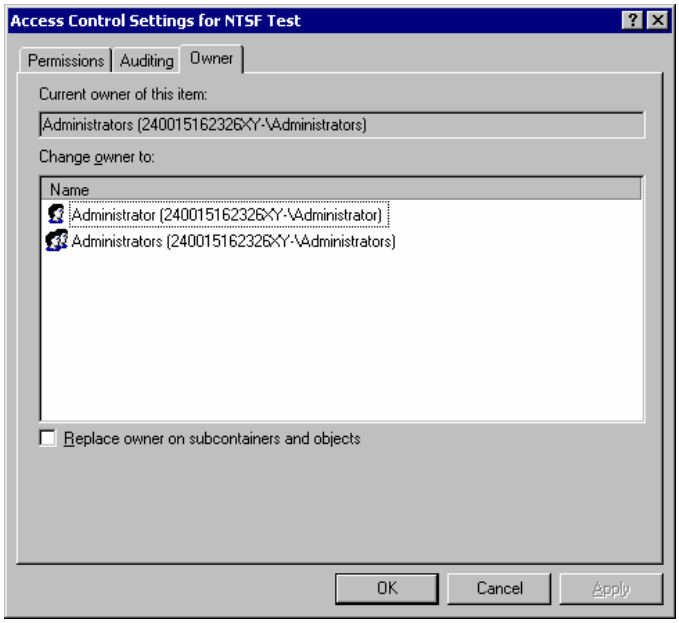

Figure 49: Access Control Settings, Owner tab dialog box for folder name NTSF Test

The current owner of the file or folder is listed at the top of the screen. To take ownership:

1. Select the appropriate user or group from the **Change owner to** list.
2. If it is also necessary to take ownership of subfolders and files, enable the **Replace owner on subcontainers and objects** box.
3. Click **OK** to execute the commands.

Share Management

There are several ways to set up and manage shares. The WebUI provides screens for setting up and managing shares. Additional methods include using a command line interface, Windows Explorer, or NAS Management Console. This guide demonstrates using the WebUI to set up and manage shares.

As previously mentioned, the file sharing security model of the NAS device is based on the NTFS file-level security model. Share security seamlessly integrates with file security. In addition to discussing share management, this section discusses share security. See "Managing File Level Permissions" earlier in this chapter for information on file security.

Shares management topics include:

- Share Considerations
- Defining Access Control Lists
- Integrating Local File System Security into Windows Domain Environments
- Comparing Administrative and Standard Shares
- Planning for Compatibility between File-Sharing Protocols
- Managing Shares

Share Considerations

Planning the content, size, and distribution of shares on the NAS 1000s can improve performance, manageability, and ease of use.

The content of shares should be carefully chosen to avoid two common pitfalls: either having too many shares of a very specific nature or of having very few shares of a generic nature. For example, shares for general usage are easier to set up in the beginning, but can cause problems later. Frequently, a better approach is to create separate shares with a specific purpose or group of users in mind. However, creating too many shares also has its drawbacks. Take care to avoid creating shares unnecessarily. For example, if it is sufficient to create a single share for user home directories, create a "homes" share rather than creating separate shares for each user.

By keeping the number of shares and other resources low, the performance of the NAS 1000s is optimized. For example, instead of sharing out each individual user's home directory as its own share, share out the top level directory and let the users map personal drives to their own subdirectory.

Defining Access Control Lists

The Access Control List (ACL) contains the information that dictates which users and groups have access to a share, as well as the type of access that is permitted. Each share on an NTFS file system has one ACL with multiple associated user permissions. For example, an ACL can define that User1 has read and write access to a share, User2 has read only access, and User3 has no access to the share. The ACL also includes group access information that applies to every user in a configured group. ACLs are also referred to as permissions.

Integrating Local File System Security into Windows Domain Environments

ACLs include properties specific to users and groups from a particular workgroup server or domain environment. In a multidomain environment, user and group permissions from several domains can apply to files stored on the same device. Users and groups local to the NAS 1000s can be given access permissions to shares managed by the device. The domain name of the NAS 1000s supplies the context in which the user or group is understood. Permission configuration depends on the network and domain infrastructure where the server resides.

File-sharing protocols (except NFS) supply a user and group context for all connections over the network. (NFS supplies a machine based context.) When new files are created by those users or machines, the appropriate ACLs are applied.

Configuration tools provide the ability to share permissions out to clients. These shared permissions are propagated into a file system ACL and when new files are created over the network, the user creating the file becomes the file owner. In cases where a specific subdirectory of a share has different permissions from the share itself, the NTFS permissions on the subdirectory apply instead. This method results in a hierarchical security model where the network protocol permissions and the file permissions work together to provide appropriate security for shares on the device.

Note: Share permissions and file level permissions are implemented separately. It is possible for files on a file system to have different permissions from those applied to a share. When this situation occurs, the file level permissions override the share permissions.

Comparing Administrative (Hidden) and Standard Shares

CIFS supports both administrative shares and standard shares. Administrative shares are shares with a last character of $. Administrative shares are not included in the list of shares when a client browses for available shares on a CIFS server. Standard shares are shares that do not end in a $ character. Standard shares are listed whenever a CIFS client browses for available shares on a CIFS server.

The NAS 1000s supports both administrative and standard CIFS shares. To create an administrative share, end the share name with the $ character when setting up the share. Do not type a $ character at the end of the share name when creating a standard share.

Planning for Compatibility between File Sharing Protocols

When planning for cross-platform share management on the NAS 1000s, it is important to understand the different protocols and their associated constraints. Each additional protocol that is supported adds another level of constraints and complexity.

NFS Compatibility Issues

Of the file sharing protocols that are supported on the NAS 1000s, NFS introduces the most constraints. When planning to manage CIFS and NFS shares, consider two specific requirements.

Note: Further information, including details about the NFS Service and the User Mapping service, is available in Chapter 6, UNIX File System Management.

- **NFS service does not support spaces in the names for NFS file share**s.

  NFS translates any spaces in an export into an underscore character. Additional translations can be set up for files. See the "OEM Supplemental Help" chapter of the SFU help, found on the NAS 1000s. This feature is designed to ensure the greatest level of compatibility with NFS clients, because some do not work with NFS exports that contain a space in the export name.

  If you plan to use the same name when sharing a folder through CIFS, and then exporting it through NFS, do not put spaces in the CIFS share name.

- **NFS service does not support exporting a child folder when its parent folder has already been exported**.

  An NFS client can access a child folder by selecting the parent folder and then navigating to the child folder. If strict cross-platform compatibility is an administration goal, CIFS must be managed in the same way. Do not share a folder through CIFS if the parent folder is already shared.

Managing Shares

Shares can be managed through the **Shares** menu option of the WebUI. Tasks include:

- Creating a new share
- Deleting a share
- Modifying share properties

Each of these tasks is discussed in this section.

Creating a New Share

To create a new share:

1. From WebUI main menu, select the **Shares** directory and then select the **Shares** option. The **Shares** dialog box is displayed. From the **Shares** dialog box, click **New**. The **General** tab of the **Create a New Share** dialog box is displayed.

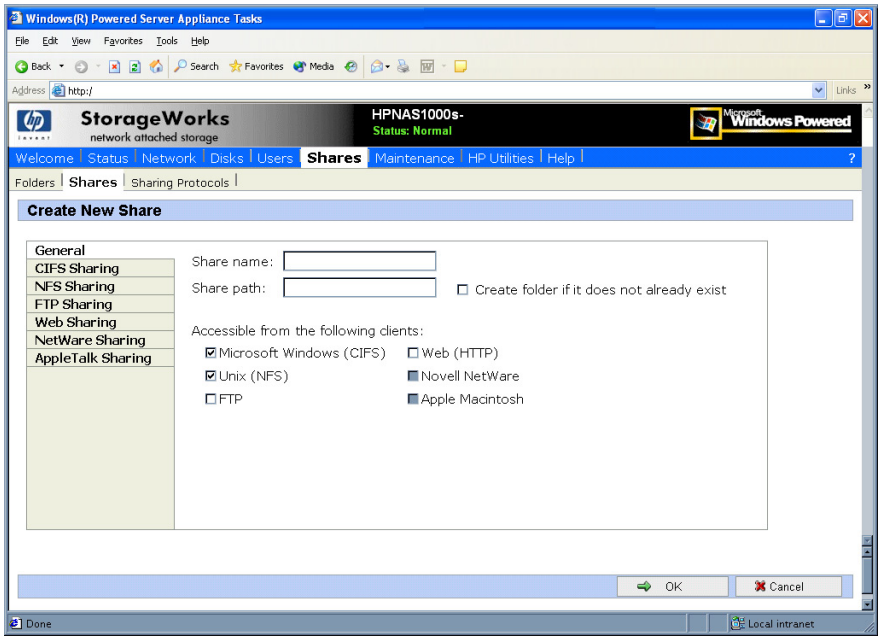

Figure 50: Create a New Share dialog box, General tab

2. Enter the following information:
   - Share name
   - Share path
   - Client protocol types

   To create a folder for the new share, check the indicated box and the system will create the folder at the same time it creates the share.

   Protocol specific tabs are available to enter sharing and permissions information for each sharing type. See "Modifying Share Properties" for detailed information on these tabs.
3. After entering all share information, click **OK**.

Deleting a Share

Caution: Before deleting a share, warn all users to exit that share and confirm that no one is using the share.

To delete a share:

1. From the **Shares** menu, click **Delete**.
2. Verify that this is the correct share, and then click **OK**.

Note: This option deletes only the share. The resource is not deleted.

Modifying Share Properties

To change share settings:

1. From the **Shares** menu, select the share to modify and then click **Properties**. The **General** tab of the **Share Properties** dialog box is displayed.

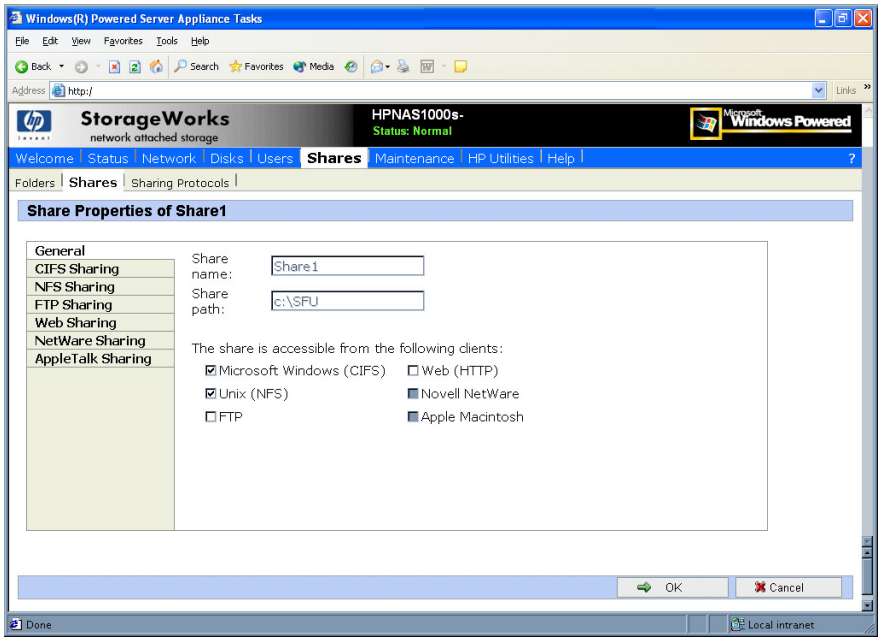

Figure 51: Share Properties dialog box, General tab

The name and path of the selected share is displayed.

2. To enter or change client protocol information, check the appropriate boxes and then click the corresponding tabs.
   - CIFS Sharing
   - NFS Sharing
   - FTP Sharing
   - Web Sharing (HTTP)
   - NetWare Sharing (NCP)
   - AFP (AppleTalk) Sharing

   Each of these tabs is discussed in the following paragraphs.
3. After all share information has been entered, click **OK**. The **Share** menu is displayed again.

CIFS Sharing

From the **CIFS Sharing** tab of the **Share Properties** dialog box:

1. Enter a descriptive **Comment**, and the **User limit** (optional).

   See Figure 52 for an example of the **CIFS Sharing** tab screen display.
2. If file caching on the client machines is allowed, click **Enable file caching on client computers accessing this share**.

Select one of the following caching policies:

- **Manual Caching for Documents**—The default setting. Recommended for folders containing user documents. Users must manually specify any files that they want available when working offline. To ensure proper file sharing, the server version of the file is always open.
- **Automatic Caching for Documents**—Also recommended for folders containing user documents. In contrast to the default setting of Manual Caching, with this option, open files are automatically downloaded and made available when working offline. Older copies are automatically deleted to make room for newer, more recently accessed files. To ensure proper file sharing, the server version of the file is always open.
- **Automatic Caching for Programs**—Recommended for folders with read only data or run from the network applications. File sharing is not ensured. Open files are automatically downloaded and made available when working offline. Older copies are automatically deleted to make room for newer, more recently accessed files.

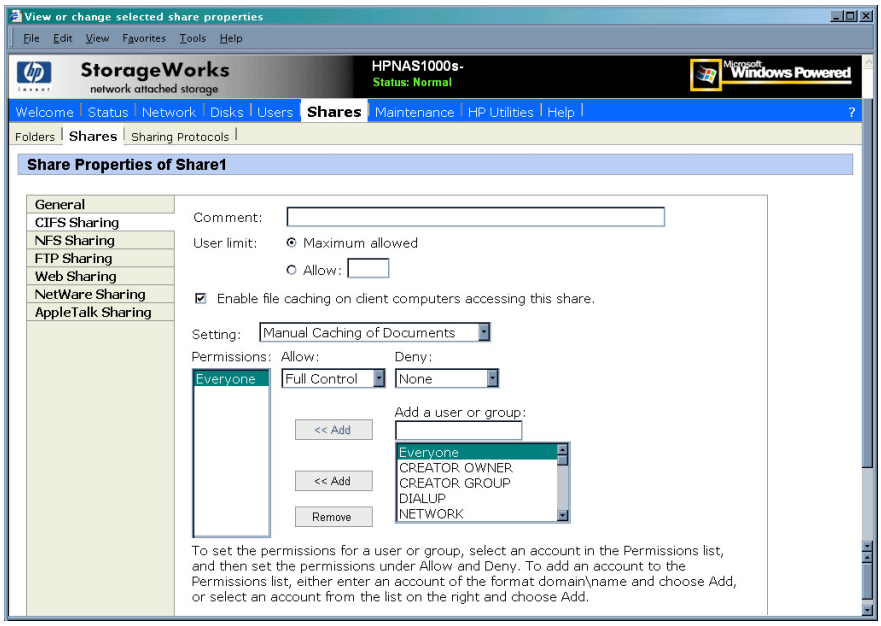

Figure 52: Share Properties dialog box, CIFS Sharing tab

3. Enter Permissions information:

   The **Permissions** box lists the currently approved users for this share.

   - *To add a new user or group*, either select a user or group from the box at the bottom right of the screen or manually enter the user or group name in the Add a user or group box and then click Add. That user or group is added to the Permissions box.
   - *To remove access to a currently approved user or group*, select the user or group from the Permissions box and then click Remove.
   - *To indicate the type of access allowed for each user*, select the user and then expand the Allow and Deny drop down boxes. Select the appropriate option.

4. After all CIFS Sharing information is entered, either click the next **Sharing** tab or click **OK**.

NFS Sharing

From the **NFS Sharing** tab of the **Create a New Share** dialog box:

1. Indicate the machines that will have access to this share.

   Select the machine to include in the **Select a client or client group** box or manually enter the NFS client computer name or IP address. Then click **Add**.

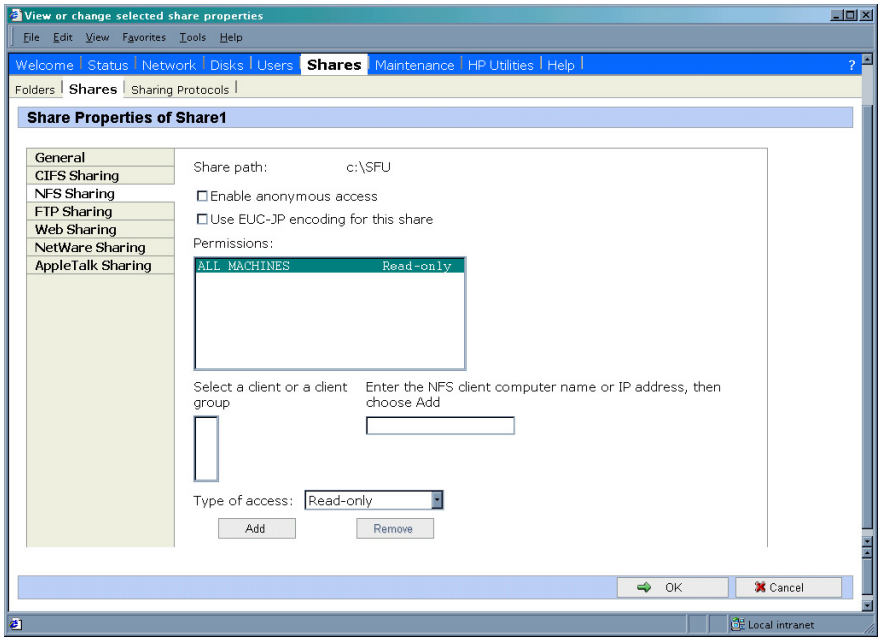

Figure 53: Share Properties dialog box, NFS Sharing tab

2. Indicate whether to allow anonymous access to the NFS share.
3. Indicate the permissions.

   Select the machine from the main user display box, and then select the appropriate access methods from the Type of access drop down box at the bottom of the screen.
4. After all NFS sharing information is entered, either click the next **Sharing** tab or click **OK**.

FTP Sharing

From the **FTP Sharing** tab of the **Create a New Share** dialog box:

1. Select the read and write access permissions that are allowed, and indicate whether visits should be written to the FTP log.
2. Then, either click the next **Sharing** tab or click **OK**.

Web Sharing (HTTP)

From the **Web Sharing** tab of the **Create New Share** dialog box:

1. Select the read and write access permissions that are allowed, and indicate whether visits should be written to the HTTP log.
2. Then, either click the next **Sharing** tab or click **OK**.

NetWare Sharing (NCP)

Note: NCP shares can be set up only after Microsoft Services for NetWare (SFN) has been installed on the NAS 1000s. Procedures for installing SFN are included in Chapter 7, NetWare File System Management.

From the **NetWare Sharing** tab, as illustrated in Figure 54, of the Create a New Share dialog box:

1. Enter a user limit.
2. Enter Permissions information.

   The **Permissions** box lists the currently approved users for this share.

   - *To add a new user or group*, either select a user or group from the box at the bottom right of the screen or manually enter the user or group name in the **Add a user or group** box. Then click **Add**. That user or group is added to the **Permissions** box.
   - *To remove access to a currently approved user or group*, select the user or group from the **Permissions** box, and then click **Remove**.
   - *To indicate the allowed access for each user*, select the user and then expand the **Allow** and **Deny** drop down boxes. Then, select the appropriate option.
3. After all NetWare Sharing information is entered, either click the next **Sharing** tab or click **OK**.

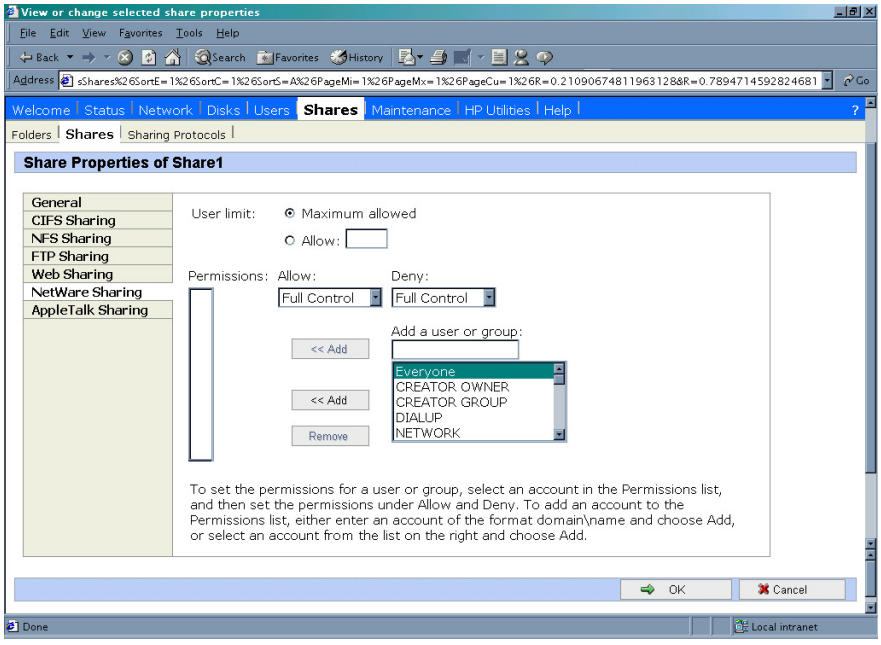

Figure 54: Share Properties dialog box, NetWare Sharing tab

AFP (AppleTalk) Sharing

AppleTalk shares can be set up only after Service for AppleTalk and Microsoft Windows NT Services for Macintosh have been installed on the NAS 1000s.

Installing Services for AppleTalk

To install Services for AppleTalk:

1. From the desktop of the NAS 1000s, click **Start**, navigate to **Settings-Network and Dial-up Connections**, click **Local Area Connection**, and then click **Properties**.
2. Click **Install**. The **Select Network Component Type** dialog box is displayed.

   Figure 55 is an example of the **Select Network Component Type** dialog box.

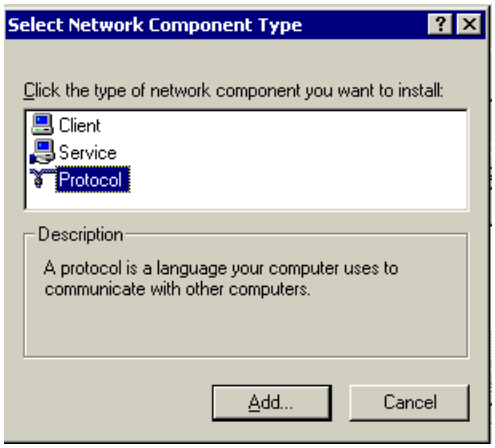

Figure 55: Local Area Connection Properties page, Install option

3. Select **Protocol** and click **Add**.
4. Select **AppleTalk Protocol** and click **OK**.

Installing Windows NT Services for Macintosh

To install Windows NT Services for Macintosh:

1. Select **Maintenance** from the WebUI interface.
2. Select **Terminal Services**.
3. Open **Add/Remove Programs** from the Control Panel.
4. Click **Add/Remove Windows Components**.
5. Double-click **Other Network File and Print Services**.
6. Select **File Services for Macintosh** then click **OK**.
7. Click **Next**.
8. Click **Finish**.

To set up AppleTalk shares, from the **AppleTalk Sharing** tab of the **Create a New Share** dialog box:

1. Enter a user limit.
2. Enter password information.
3. Indicate whether the share has read only permission or read write permission.
4. After all AFP (AppleTalk) Sharing information is entered, either click the next **Sharing** tab or click **OK**.

Protocol Parameter Settings

As previously mentioned, the NAS 1000s supports the following protocols:

- CIFS
- NFS
- FTP
- HTTP
- NCP (NetWare)
- AFP (AppleTalk)

This section discusses the parameter settings for each protocol type.

To access and enter protocol parameter settings:

1. From the **Shares** menu, select **Sharing Protocols**. The **File Sharing Protocols** dialog box is displayed.

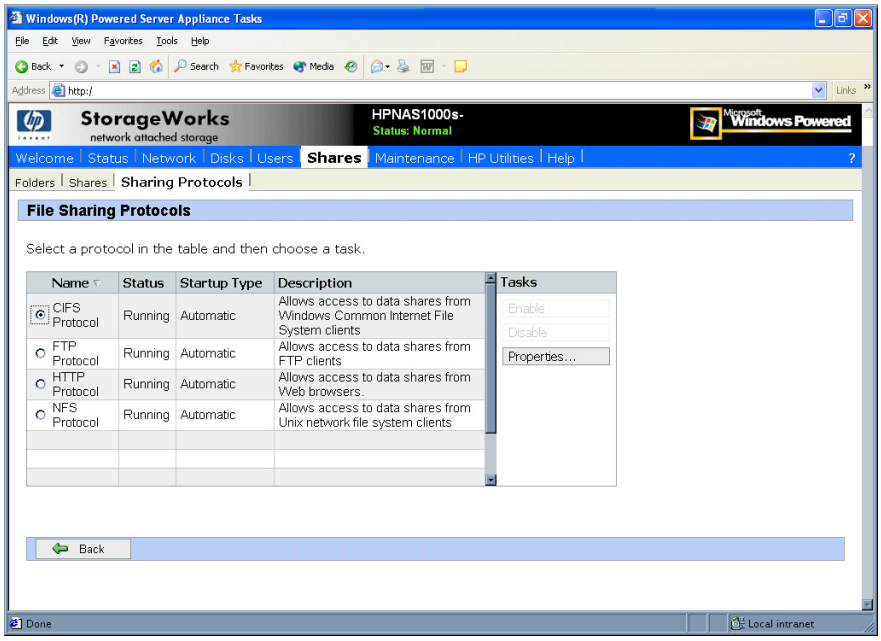
Windows(R) Powered Server Appliance Tasks
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http:/
Links
StorageWorks
network attached storage
HPNAS1000s-
Status: Normal
Microsoft Windows Powered
Welcome Status Network Disks Users Shares Maintenance HP Utilities Help ?
Folders Shares Sharing Protocols
File Sharing Protocols
Select a protocol in the table and then choose a task.
Name Status Startup Type Description
CIFS Protocol Running Automatic Allows access to data shares from Windows Common Internet File System clients
FTP Protocol Running Automatic Allows access to data shares from FTP clients
HTTP Protocol Running Automatic Allows access to data shares from Web browsers
NFS Protocol Running Automatic Allows access to data shares from Unix network file system clients
Tasks
Enable
Disable
Properties...
Back
Done
Local intranet

Figure 56: Sharing Protocols dialog box

2. Protocols and their statuses are listed. The following options are available:
   - Enabling a protocol
   - Disabling a protocol
   - Modifying Protocol Settings

Because enabling and disabling a protocol are self explanatory, only modifying protocol specific settings is described in this section.

CIFS Protocol Settings

There are no user configurable settings for CIFS.

NFS Protocol Settings

NFS is the networking protocol for exporting UNIX file systems across a network. UNIX and NFS are discussed in Chapter 6, UNIX File System Management.

Some of the NFS protocol settings include:

- Async/Sync Settings
- Locks
- Client Groups
- User and Group Mappings

FTP Protocol Settings

Three tabs are presented in the FTP Protocol Properties dialog box: **Logging**, **Anonymous Access**, and **Messages**.

Within these tabs:

- **Logging**—Enable logging
- **Anonymous Access**—Enable anonymous access
- **Messages**—Enter a welcome and an exit message

HTTP Protocol Settings

The following parameters can be set for Web protocols:

- Indicate which IP addresses can be used to access data shares
- Indicate which port can be used to access data shares

NCP (NetWare) Protocol Settings

There are no user configurable settings for NCP.

AFP (AppleTalk) Protocol Settings

Several parameters can be set for AFP shares, including:

- Welcome message
- Security settings
- Limits on number of sessions

UNIX File System Management

6

Microsoft Services for UNIX (SFU) is a comprehensive software package designed to provide complete UNIX environment integration into a Windows NT, Windows 2000, or Active Directory domain file server. SFU manages tasks on both Windows and UNIX platforms. Tasks include creating NFS exports from Windows and administering user name mappings. SFU also includes Telnet Server and Remote Shell for remote administration.

The following SFU components are included in the NAS 1000s:

- Server for NFS
- User Name Mapping
- Telnet and Remote Shell Services
- Password Synchronization

The following topics are described in this chapter:

- Network File System
- Server for NFS
  - Authenticating User Access
  - Indicating the Computer to Use for the NFS User Mapping Server
  - Logging Events
  - Installing NFS Authentication Software on the Domain Controller
- NFS File Shares
- NFS Protocol Properties Settings
- NFS Client Groups
  - Adding a New Client Group
  - Deleting a Client Group
  - Editing Client Group Information
- NFS User and Group Mappings
  - Types of Mappings
  - User Name Mapping Best Practices
  - Creating and Managing User and Group Mappings
  - Backing up and Restoring Mappings

- NFS File Sharing Tests
- Terminal Services, Telnet Service, and Remote Shell Service
  - Using Terminal Services
  - Using Telnet Service
  - Using Remote Shell Service
- Password Synchronization

Network File System

Network File System (NFS) is a networking protocol for exporting UNIX file systems across a network.

There are two versions of NFS, Version 2 and Version 3. Version 3 supports additional file operations that Version 2 did not have.

In addition, NFS has the capacity to operate with two different network protocols, Transport Control Protocol (TCP) and User Datagram Protocol (UDP).

Traditionally, NFS operates with UDP for performance purposes, but it can also operate with TCP.

There are three key design goals of NFS:

- Allow different UNIX machines to transparently export files across a network.

  This feature works across different versions of UNIX and across different platforms. For example, a Linux machine can access files on a Tru64™ UNIX machine. Accessing these files is transparent to both the administrator and the users. The administrator and user do not notice any difference between accessing local files or files on the remote machine.
- Make the administration as easy as possible.

  The remote file system connects to the local machine in the same manner that a local file system does. The administrator is able to add a remote file system in the same manner as adding another hard drive or external storage.
- Focus exclusively on file system operations.

  The file system is used only for exporting file systems to remote machines. NFS supports only operations such as read, write, create, delete, and copy.

Server for NFS

Until recently, UNIX used only NFS to export files. UNIX based platforms and Windows based platforms were not able to share files. This restriction caused UNIX clients to require UNIX file servers and Windows clients to require Windows file servers. Windows and UNIX were separate environments, including the duplication of hardware, overhead, and effort. UNIX clients can now use Windows based machines as file servers using Microsoft Services for UNIX (SFU).

SFU enables UNIX clients to use Windows based machines as file servers. The SFU NFS server supports NFS Version 2 and Version 3, and supports them both on the TCP and UDP network protocols.

SFU is more fully integrated into the operating system than other third party NFS server packages. The administrative interface for NFS exports is similar to the Common Internet File System (CIFS) sharing interface used by Windows platforms.

Authenticating User Access

NFS export access is granted or denied to clients based on client name or IP address. The server determines whether a specific client machine has access to an NFS export. No user logon to the NFS server takes place when a file system is exported by the NFS server. Permission to read or write to the export is granted to specific client machines. For example, if client machine M1 is granted access to an export but client M2 is not, user jdoe can access the export from M1 but not from M2.

Permissions are granted on a per-export basis; each export has its own permissions, independent of other exports on the system. For example, file system a can be exported to allow only the Accounting department access, and file system m can be exported allowing only the Management department access. If a user in Management needs access to the Accounting information, the a export permissions can be modified to let that one user's client machine have access. This modification does not affect other client access to the same export, nor does it allow the Management user or client access to other exports.

After the client machine has permission to the export, the user logon affects file access. The client machine presents the UNIX user ID (UID) and group ID (GID) to the server. When the computer accesses a file, the user logon is compared against the typical UNIX permissions of user, group, and other, and typical UNIX access is applied.

Note: User credentials are not questioned or verified by the NFS server. The server accepts the presented credentials as valid and correct.

If the NFS server does not have a corresponding UID or GID, or if the administrator has set other conditions to filter out the user, a process called squashing takes effect. Squashing is the conversion of an unknown or filtered user to an anonymous user. This anonymous user has very restricted permissions on the system. Squashing helps administrators manage access to their exports by allowing them to restrict access to certain individuals or groups and to squash all others down to restricted (or no) access. Squashing enables the administrator to allow permissions instead of denying access to all the individuals who are not supposed to have access. See "NFS User and Group Mappings" later in this chapter for specific information about creating and maintaining mappings.

Indicating the Computer to Use for the NFS User Mapping Server

During the processes of starting and installing the NAS 1000s, the name localhost is assigned by default to the computer. It is assumed that the NAS 1000s is the computer that will be used for user name mapping.

If there are other mapping servers and a machine other than the localhost that will store user name mappings, the name of that computer must be indicated, as detailed below:

1. Use Terminal Services to access the **NAS Management Console**, click **File Sharing**, **Services for UNIX**. Click **Server for NFS**. Figure 57 is an example of the Server for NFS user interface.
2. In the **Computer** name box of the user-mapping screen, type the name of the computer designated for user mapping and authentication.
3. Localhost is the computer name assigned by default on the NAS 1000s. To control user mapping from a different computer, enter the name of that computer.

Note: If a machine other than the localhost is to be used, make sure that the user name mapping service is installed and running on that machine.

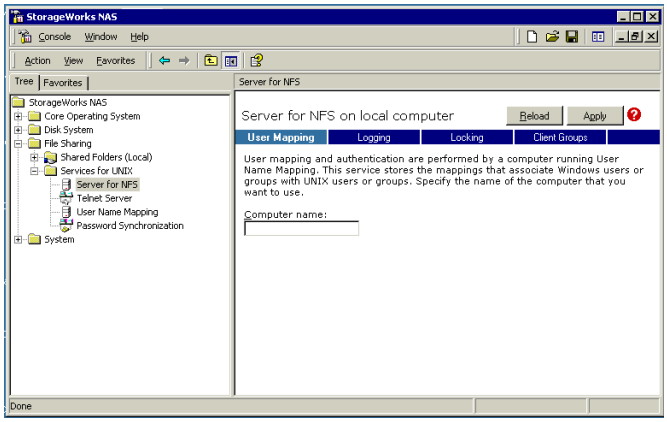

Figure 57: NAS Management Console Server for NFS screen, User Mapping tab

Logging Events

Various levels of auditing are available. Auditing sends SFU events to a file for later review and establishes log-setting behavior. Some behavior examples include events logged and log file size. See the online SFU help for more information.

1. Use Terminal Services to access the NAS Management Console, click **File Sharing**, **Services for UNIX**, **Server for NFS**. Click the **Logging** tab.
2. To log events to the event viewer application log, click the check box for **Log events to event log**.
3. To log selected event types, click the check box for **Log events in this file** on the screen.
4. Enter a filename or use the default filename provided (*rootdrive\SFU\log\nfssvr.log*) and log file size (7-MB default). The default log file is created when the changes are applied.

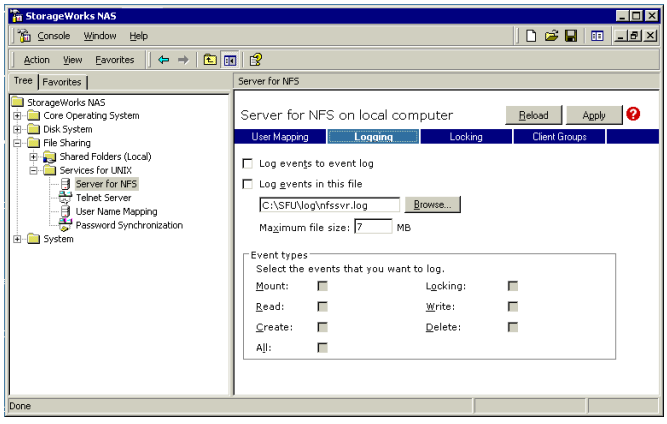

Figure 58: NAS Management Console Server for NFS screen, Logging tab

Installing NFS Authentication Software on the Domain Controllers and Active Directory Domain Controllers

The NFS Authentication software must be installed on all Primary Domain Controllers (PDCs) and backup domain controllers (BDCs) that have Windows users mapped to UNIX users. This includes active directory domains. For instructions on setting up user mappings, see "NFS User and Group Mappings."

To install the Authentication software on the domain controllers:

1. Locate the *sfucustom.msi* file located in the *SFU* directory of the NAS 1000s.
2. Share out the *SFU* directory on the NAS 1000s.
3. On the domain controller where the service is being installed, using Windows Explorer:
   a. Connect to the SFU share on the NAS 1000s.
   b. Open the shared directory containing *sfucustom.msi*.
   c. Double-click the file to open it. Windows Installer is opened.

Note: If the domain controller being used does not have Windows Installer installed, locate the file InstMSI.exe on the SFU directory and run it. After this installation, the Windows Installer program starts when opening sfucustom.msi.

---

   d. Click **Next** when the Welcome screen is displayed.
   e. Enter the **User name** and **Organization** and click **Next**.
   f. Accept the license agreement and click **Next**.
   g. Select **Customized Installation** and click **Next**.
   h. Mark the selections to add **Authentication Tools for NFS** and de-select **Password Synchronization**. To de-select **Password Synchronization**, expand the drop down box and select the red "**X**" next to **Password Synchronization**. (The entire feature will be unavailable.) The instructions for installing both Authentication Tools for NFS and Password Synchronization are found later in this chapter.
   i. Select the installation directory and click **Next**.
   j. Click **Finish** when installation is complete.

NFS File Shares

NFS file shares are created in the same manner as other file shares, however there are some unique settings. Procedures for creating and managing NFS file shares are documented in the same sections as creating file shares for other protocols. See the "Folder and Share Management" chapter for more information.

Note: NFS specific information is extracted from Chapter 5, Folder and Share Management, and duplicated below.

Complete share management is performed through the **Shares** menu option of the WebUI. Tasks include:

- Creating a new share
- Deleting a share
- Modifying share properties

Each of these tasks is discussed in this section.

Creating a New Share

To create a new NFS file share:

1. From the WebUI main menu, select the **Shares** directory and then select the **Shares** option. The **Shares** dialog box is displayed. From the **Shares** dialog box, click **New**. The **General** tab of the **Create a New Share** dialog box is displayed.

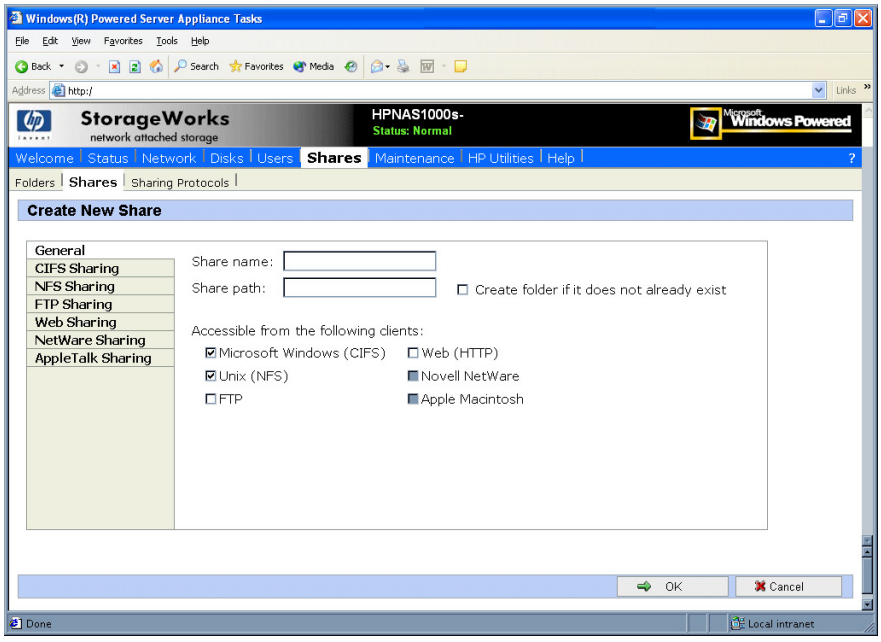

Figure 59: Create a New Share dialog box, General tab

2. In the **General** tab, enter the share name and path. Check the **Unix (NFS)** client protocol check box.

Note: Uncheck the Microsoft Windows (CIFS) option if you do not want to allow CIFS access to the share.

Note: NFS service does not support the use of spaces in the names for NFS file shares. NFS translates any spaces in an export into an underscore character. If you plan to use the same name when sharing a folder through CIFS, and then exporting it through NFS, do not put spaces in the CIFS share name.

To create a folder for the share, check the indicated box and the system will create the folder at the same time it creates the share.

3. Select the **NFS Sharing** tab to enter NFS specific information. See "Modifying Share Properties" for information on this tab.
4. After all share information is entered, click **OK**.

Deleting a Share

Caution: Before deleting a share, warn all users to exit that share. Then confirm that no one is using the share.

To delete a share:

1. From the **Shares** menu, select the share to be deleted, and then click **Delete**.
2. Verify that this is the correct share, and then click **OK**.

Modifying Share Properties

To change share settings:

1. From the **Shares** menu, select the share to modify and then click **Properties**. The **General** tab of the **Share Properties** dialog box is displayed.

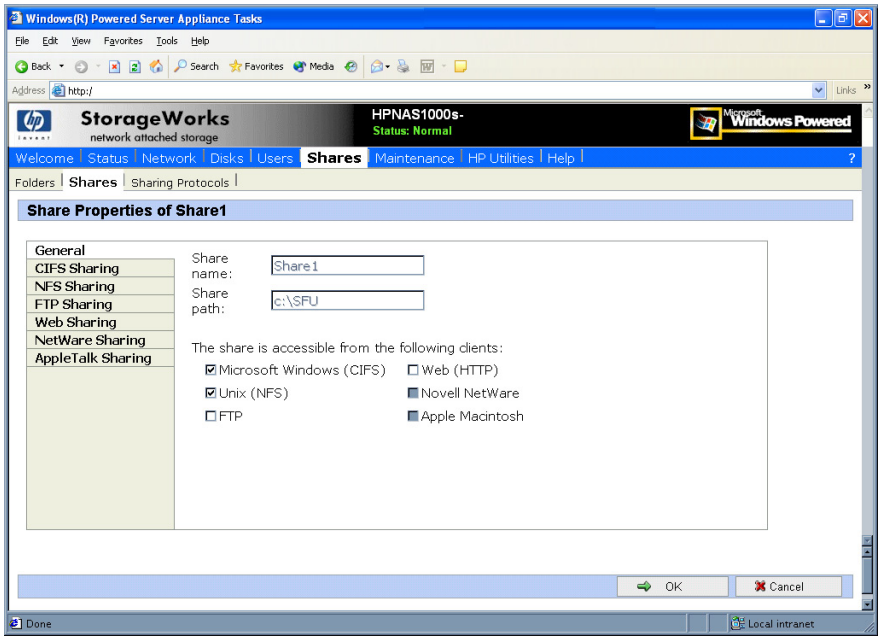

Figure 60: Share Properties dialog box, General tab

The name and path of the selected share is displayed.

2. To enter or change client protocol information, check the **UNIX (NFS)** client type box and then click the **NFS Sharing** tab.

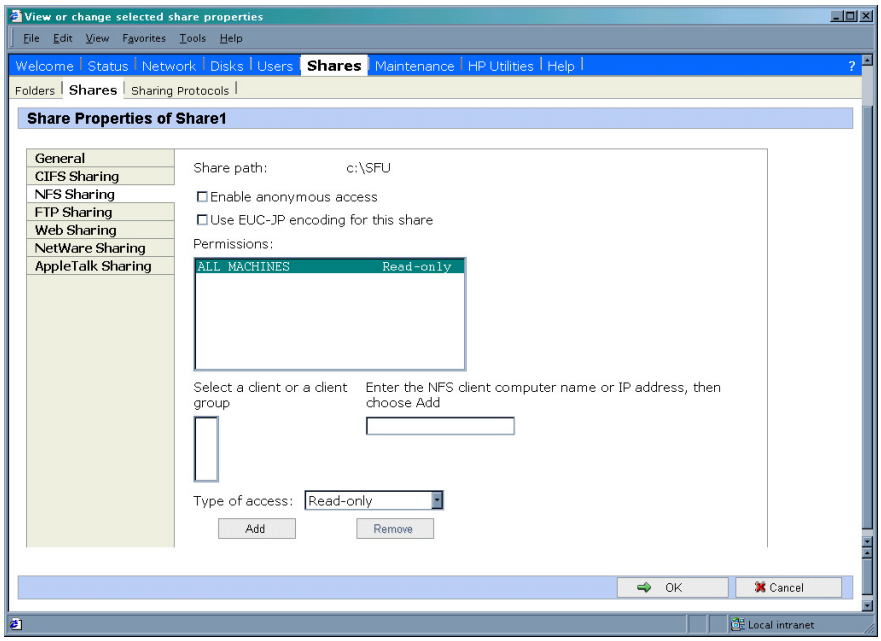

Figure 61: NFS Sharing tab

3. From the **NFS Sharing** tab of the **Share Properties** dialog box,
   a. Indicate the allowed clients.

      Select the machine to include in the **Select a client or client group** box or manually enter the NFS client computer name or IP address. Then click **Add**.

   b. Indicate whether to allow anonymous access to the NFS share.

Note: The default values for Anonymous UID and Anonymous GID are -2. Non-default IDs can be specified for the NFS share using Terminal Services.

---

   c. Indicate the access permissions.

      Select the machine from the main user display box and then select the appropriate access method from the **Type of access** drop down box.

      The types of access are:

      - **Read-only**—Use this permission to restrict write access to the share.
      - **Read-write**—Use this permission to allow clients to read or write to the share.
      - **Read-only + Root**—Use this permission to restrict write access to the share. Use this permission to assign administrative access to the share. This will allow the client computer to have root access to the NFS share. Map the UNIX root user to the Windows user Administrator. Also, map the group that this UNIX root belongs to, to the Windows group Administrator.
      - **Read-write + Root**—Use this permission to allow clients to read or write to the share. Use this permission to assign administrative access to the share. This will allow the client computer to have root access to the NFS share. Map the UNIX root user to the Windows user Administrator. Also, map the group that this UNIX root belongs to, to the Windows group Administrator.
      - **No access**—Use this permission to restrict all access to the share.

4. After all NFS sharing information is entered, click **OK**.

Encoding Types

Two encoding types can be selected using the WebUI. These include the default ANSI as well as EUC-JP. Other encoding types can be assigned to the NFS share using Terminal Services. The encoding choices are:

- ANSI (default) - able to assign with the WebUI
- BIG5 (Chinese)
- EUC-JP (Japanese) - able to assign with the WebUI
- EUC-KR (Korean)
- EUC-TW (Chinese)
- GB2312-80 (Simplified Chinese)
- KSC5601 (Korean)
- SHIFT-JIS (Japanese)

If the option is set to ANSI on systems configured for non-English locales, the encoding scheme is set to the default encoding scheme for the locale. The following are the default encoding schemes for the indicated locales:

- Japanese: SHIFT-JIS
- Korean: KS C 5601-1987
- Simplified Chinese: GB
- Traditional Chinese: BIG5

NFS Protocol Properties Settings

Parameter settings for the NFS protocol are entered and maintained through the WebUI in the **NFS Properties** dialog box. To access the **NFS Properties** dialog box, select **Shares**, **Sharing Protocols**. Then, select the **NFS Protocol** radio button and click **Properties**.

The **NFS Properties** menu is displayed.

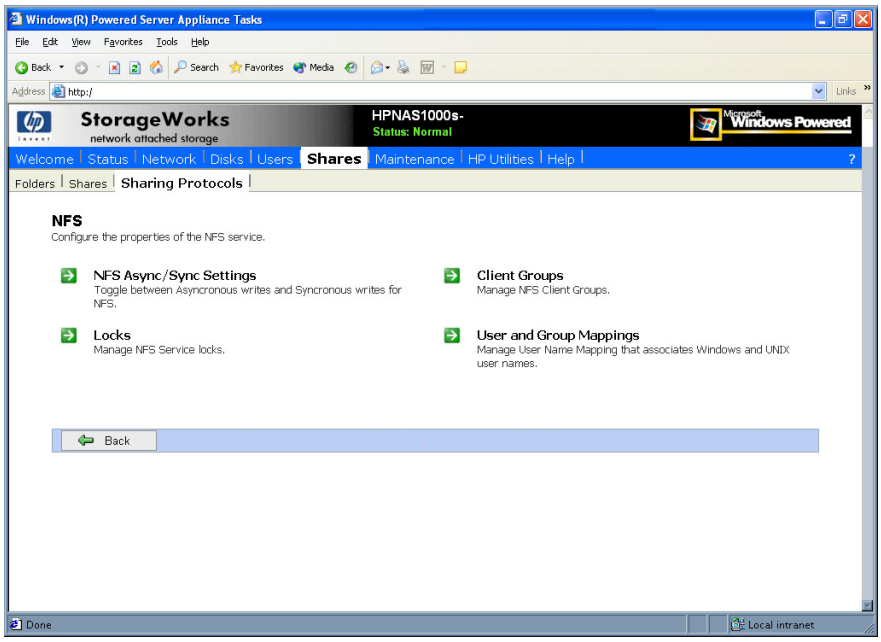

Figure 62: NFS Sharing Protocols menu

NFS properties include:

- Async/Sync Settings
- Locks
- Client Groups
- User and Group Mappings

Settings for asynchronous/synchronous writes and service locks are discussed together in the following paragraphs of this chapter.

Client groups and user and group mappings are each discussed in separate sections later in this chapter.

NFS Async/Sync Settings

As mentioned in a previous section, there are two versions of NFS: Version 2 and Version 3. Version 3 supports additional file operations that Version 2 did not have, such as asynchronous file operations.

To indicate whether to use asynchronous or synchronous write settings:

1. From the WebUI, access the **NFS Protocol Properties** menu by selecting **Shares**, **Sharing Protocols**. Select **NFS Protocol** and then click **Properties**. The **NFS Properties** menu is displayed.
2. In the **NFS Properties** menu, select **NFS Async/Sync Settings**. The **NFS Async/Sync Settings** dialog box is displayed.
3. Select the desired write setting. The default setting is Synchronous writes.

Note: Using synchronous writes allows for greater data integrity. Asynchronous writes will increase performance but will reduce data integrity as the data is cached before being written to disk.

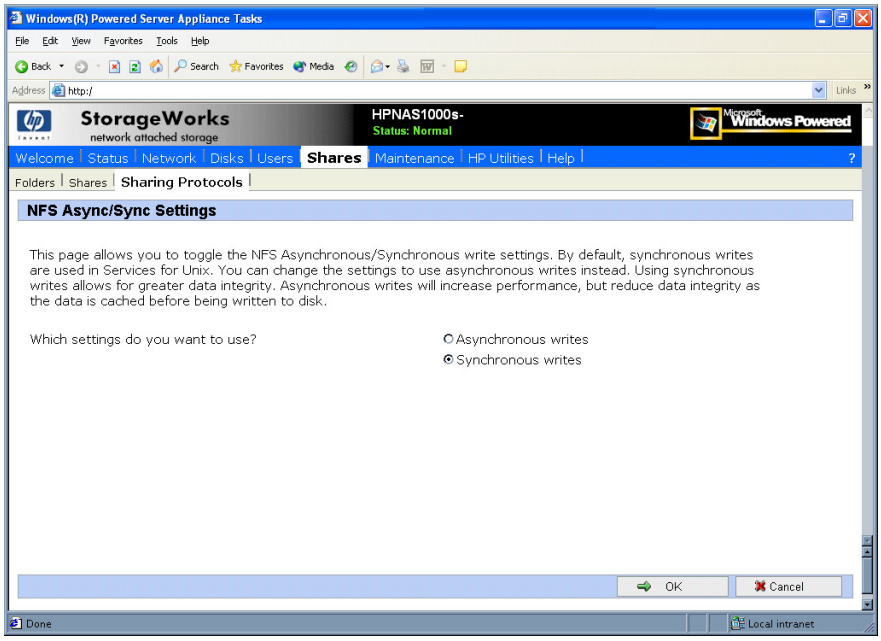
Windows(R) Powered Server Appliance Tasks
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http:/
Links
StorageWorks
network attached storage
HPNAS1000s-
Status: Normal
Microsoft Windows Powered
Welcome Status Network Disks Users Shares Maintenance HP Utilities Help
Folders Shares Sharing Protocols
NFS Async/Sync Settings
This page allows you to toggle the NFS Asynchronous/Synchronous write settings. By default, synchronous writes are used in Services for Unix. You can change the settings to use asynchronous writes instead. Using synchronous writes allows for greater data integrity. Asynchronous writes will increase performance, but reduce data integrity as the data is cached before being written to disk.
Which settings do you want to use?
Asynchronous writes
Synchronous writes
OK
Cancel
Done
Local intranet

Figure 63: NFS Async/Sync Settings dialog box

NFS Locks

NFS supports the ability to lock files. File locking helps prevent two or more users from working with the same files at the same time.

NFS locking depends on the software application components to manage the locks. If an application does not lock a file or if a second application does not check for locks before writing to the file, nothing prevents the users from overwriting files.

To enter locking parameters:

1. From the WebUI, access the **NFS Protocol Properties** menu by selecting **Shares**, **Sharing Protocols**. Select **NFS Protocol** and then click **Properties**.

   The **NFS Properties** menu is displayed.

2. In the **NFS Properties** menu, select **Locks**. The **NFS Locks** dialog box is displayed. Figure 64 is an illustration of the **NFS Locks** dialog box.

   All clients that have locks on system files are listed in the **Current locks** box.

3. To manually clear locks that a client has on files, select the client from the displayed list, and then click **OK**.

4. To indicate the amount of time after a system failure that the locks are kept active, enter the number of seconds in the **Wait period** box.

The NAS 1000s keeps the locks active for the specified number of seconds, while querying the client to see if it wants to keep the lock. If the client responds within this time frame, the lock is kept active. Otherwise, the lock is cleared.

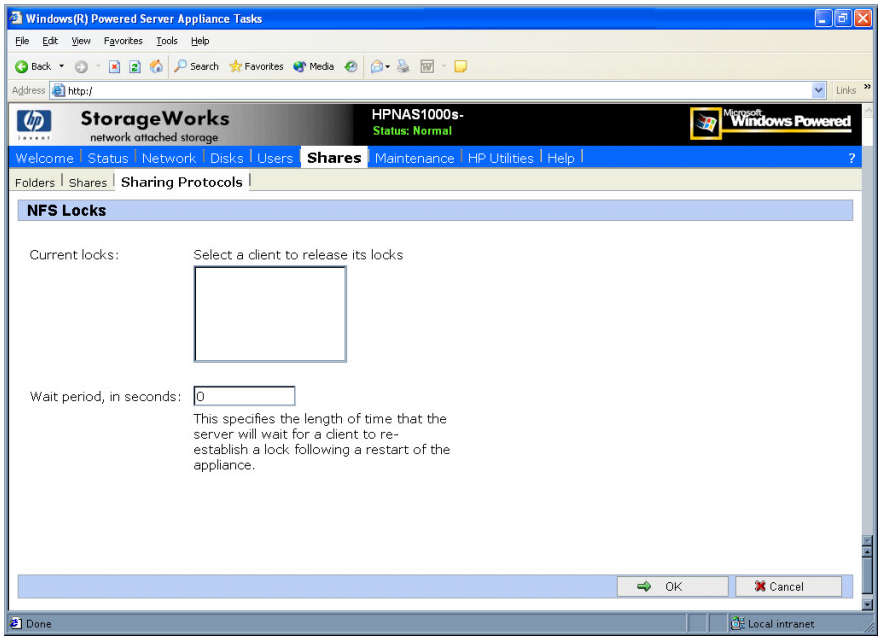
Windows(R) Powered Server Appliance Tasks
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http:/
Links
StorageWorks
network attached storage
HPNAS1000s-
Status: Normal
Microsoft Windows Powered
Welcome Status Network Disks Users Shares Maintenance HP Utilities Help ?
Folders Shares Sharing Protocols
NFS Locks
Current locks:
Select a client to release its locks
Wait period, in seconds:
0
This specifies the length of time that the server will wait for a client to re-establish a lock following a restart of the appliance.
OK
Cancel
Done
Local intranet

Figure 64: NFS Locks dialog box

NFS Client Groups

The Client Groups feature gives administrators a method of assigning access permissions to a set of clients. The administrator creates a client group, gives it a name, and then inserts clients into the group by client name or IP address. After the client group is created, the administrator adds or removes permissions for the entire group, instead of allowing or denying access for each individual client machine.

Proper planning includes control over the naming conventions of client groups and users. If the client group is given the same name as a client, the client is obscured from the view of the server. For example, assume that a client d4 exists. If a client group called d4 is created, permissions can no longer be assigned to just the client d4. Any reference to d4 now refers to client group d4.

To manage NFS client groups:

1. From the WebUI, access the **NFS Protocol Properties** dialog box by selecting **Shares**, **Sharing Protocols**. Select **NFS Protocol** and then click **Properties**. The **NFS Protocol Properties** menu is displayed.
2. In the **NFS Protocol Properties** menu, select **Client Groups**. The **NFS Client Groups** dialog box is displayed.

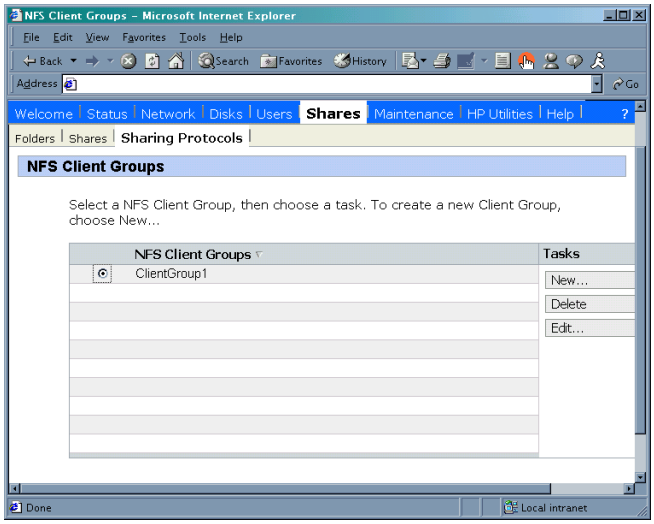

Figure 65: NFS Client Groups dialog box

The following tasks are available:

- Adding a new client group
- Deleting a client group
- Editing client group information

Adding a New Client Group

To add a new client group:

1. From the **NFS Client Groups** dialog box, click **New**. The **New NFS Client Group** dialog box is displayed.

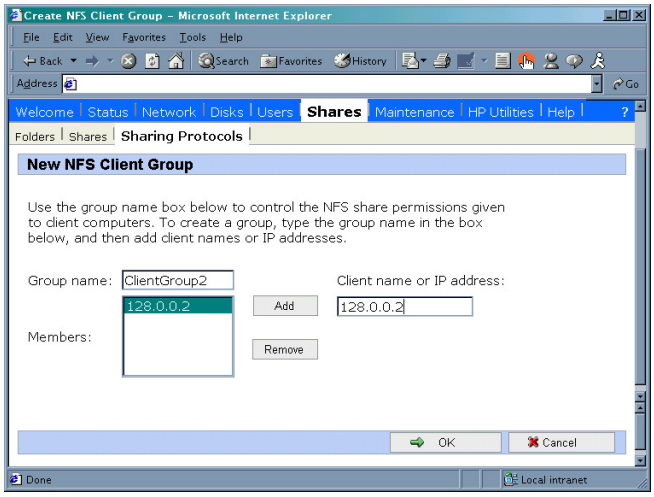
Create NFS Client Group – Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address
Go
Welcome Status Network Disks Users Shares Maintenance HP Utilities Help ?
Folders Shares Sharing Protocols
New NFS Client Group
Use the group name box below to control the NFS share permissions given to client computers. To create a group, type the group name in the box below, and then add client names or IP addresses.
Group name: ClientGroup2
Client name or IP address:
128.0.0.2
Add
128.0.0.2
Members:
Remove
OK
Cancel
Done
Local intranet

Figure 66: New NFS Client Group dialog box

2. Enter the name of the new group.
3. Enter the client name or their IP address.
4. Click **Add**. The system adds the client to the displayed list of members.
5. To remove a client from the group, select the client from the **Members** box and then click Remove.
6. After all clients have been added to the group, click **OK**. The **NFS Client Groups** dialog box is displayed again.

Deleting a Client Group

To delete a group:

1. From the **NFS Client Groups** dialog box, select the group to delete and click **Delete**.
2. A verification screen is displayed. Confirm that this is the correct group and then click **OK**.

   The **NFS Client Groups** dialog box is displayed again.

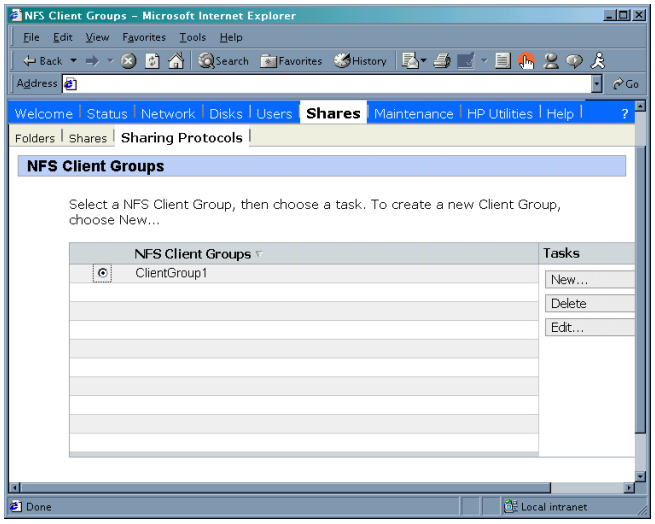

Figure 67: Client Groups dialog box

Editing Client Group Information

To modify the members of an existing client group:

1. From the **NFS Client Groups** dialog box, select the group to modify, and click **Edit.**

   The **Edit NFS Client Group** dialog box is displayed. Current members of the group are listed in the **Members** box.

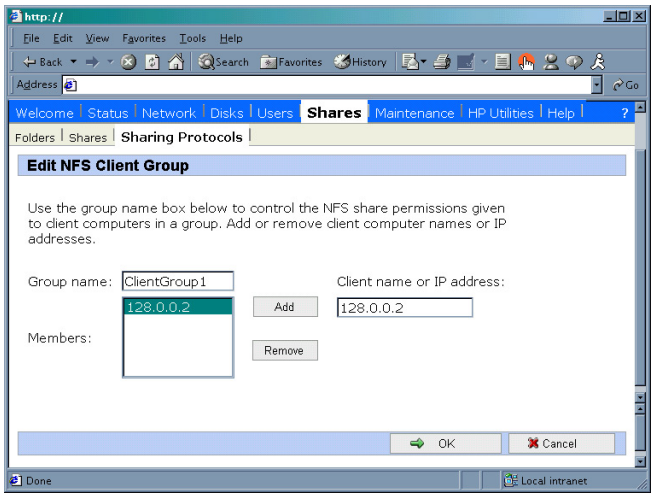

Figure 68: Edit NFS Client Groups dialog box

2. To add a client to the group, enter the client name or IP address in the **Client name** box, and then click **Add**. The client is automatically added to the **Members** list.
3. To delete a client from the group, select the client from the **Members** list, and then click **Remove**. The client is removed from the list.
4. After all additions and deletions are completed, click **OK**. The **NFS Client Groups** dialog box is displayed again.

NFS User and Group Mappings

When a fileserver exports files within a homogeneous environment, there are no problems with authentication. It is a simple matter of making a direct comparison to determine whether the user should be allowed access to the file, and what level of access to allow.

However, when a fileserver works in a heterogeneous environment, some method of translating user access is required. User mapping is the process of translating the user security rights from one environment to another.

User name mapping is the process of taking user and group identification from one environment and translating it into user identification in another environment. In the context of UNIX and NFS, user and group identification is a combination of a user ID (UID) and group ID (GID). In Windows environments, user identification is a Security ID (SID) or, in Windows 2000, a Globally Unique Identifier (GUID).

The server grants or denies access to the export based on machine name or IP address. However, after the client machine has access to the export, user-level permissions are used to grant or deny access to user files and directories.

The NAS 1000s is capable of operating in a heterogeneous environment, meaning that it is able to work with both UNIX and Windows clients. Because the files are stored in the native Windows NT file system, the server has to map the UNIX users to Windows users to determine the user access level of the files.

Note: User mapping is not designed to address existing user database problems in the existing environment. All UIDs and GIDs must be unique across all NIS (Network Information Service) domains and all user names must be unique across all Windows NT domains.

The NAS 1000s supports mappings between one or more Windows domains and one or more NIS domains. The default setup supports multiple Windows NT domains to a single NIS domain. For information about users in multiple NIS domains, refer to the Supplemental Help section in the SFU online help.

Types of Mappings

There are three types of mappings. These mappings are listed below in order of the most complex (with the greatest level of security) to the least complex (easiest to manage, but with little security):

- Explicit mappings
- Simple mappings
- Squashed mappings

Explicit Mappings

Explicit mappings are created by the administrator to link Windows and UNIX users. They override simple mappings and are used to map users on the different systems that have unique names.

Simple Mappings

Simple mapping is a direct comparison of user names on the Windows system and the UNIX system. If the names match, the user is assumed to be authentic, and appropriate share access is granted. Simple mapping is an option that the administrator must turn on if it is to be used.

Squashed Mappings

If the NFS server does not have a corresponding UID or GID or if the administrator has set other conditions to filter out the user, a process called squashing takes effect. Squashing is the conversion of an unmapped or filtered user to an anonymous user. This anonymous user has very restricted permissions on the system. Squashing helps administrators manage access to their exports by allowing them to restrict access to certain individuals or groups and to squash all others down to restricted (or no) access. Squashing enables the administrator to allow permissions instead of denying access to all the individuals who are not supposed to have access.

The default squash user on Windows is "Anonymous Logon," but this default user can be changed. For more details on how to change the default squashing user, see the "OEM Supplemental Help" chapter of the SFU help, found on the NAS 1000s.

Figure 69 is a diagram showing an example of how the mapping server works for an ls -al command.

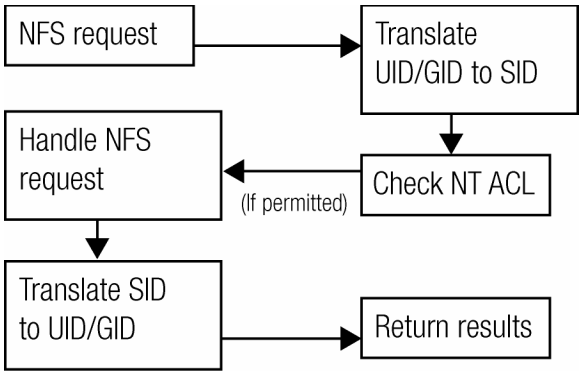

Figure 69: Mapping Server "ls -al" Command example

A double translation, as illustrated in Figure 69, is sometimes necessary because some commands return user ID information. For example, if the NFS request issued was an `ls -al` command, the return listing of files contains user information (the user and group that own the file). The `ls -al` command is a UNIX command. It returns a long or full listing of all files. Because this information is contained in a Windows NT Access Control List (ACL), it is not UNIX ready. The ACL information has to be converted back to UNIX UIDs and GIDs for the UNIX systems to understand and display the user information.

This second translation is not done for commands that do not return user information. For example, if the NFS request were just to read data from or write data to a file, the second translation would not be performed because there is no returning user information.

User Name Mapping Best Practices

This is a brief list of suggested practices:

- **Back up user and group mappings**

  To avoid loss of complex advanced mappings in the case of a system failure, back up the mappings whenever the mappings have been edited or new mappings have been added.

- **Map consistently**

  Groups that are mapped to each other should contain the same users and the members of the groups should be properly mapped to each other to ensure proper file access.

Example using User1 and Group1:

- Make sure that the Windows User1 is mapped to the corresponding UNIX User1.
- Make sure that the Windows Group1 is mapped to the corresponding UNIX Group1.
- Make sure that User1 is a member of Group1 on both Windows and UNIX.

- **Map properly**
  - Valid UNIX users should be mapped to valid Windows users.
  - Valid UNIX groups should be mapped to valid Windows groups.
  - Mapped Windows user must have the Access this computer from the Network privilege, or the mapping will be squashed.
  - The mapped Windows user must have an active password, or the mapping will be squashed.

Creating and Managing User and Group Mappings

To set up and manage user name mappings:

1. From the WebUI, select **Shares**, **Sharing Protocols**. Select **NFS Protocol** and then click **Properties**. The **NFS Properties** menu is displayed.
2. In the **NFS Properties** Menu, select **User and Group Mappings**. The **User and Group Mappings** dialog box is displayed.

   There are four tabs in the **User and Group Mappings** dialog box:

   - **General information**—Sets the mapping information source, which is either NIS or password and group files.
   - **Simple Mapping**—Indicates whether simple mappings are being used.
   - **Explicit User Mapping**—Lists exceptional user mappings that will override the simple user mappings.
   - **Explicit Group Mapping**—Lists exceptional group mappings that will override the simple group mappings.

   Each of these tabs is discussed in the following sections.
3. Enter mapping information on the appropriate tabs, then click **OK**.

General Information

The NAS 1000s stores the mapping data in an NTFS file system. The user name mapping server translates the UNIX users into Windows users so that the server can determine user access rights to the data.

Within this initial screen, indicate whether the source of mapping information is an NIS server or is a special file with password and group information.

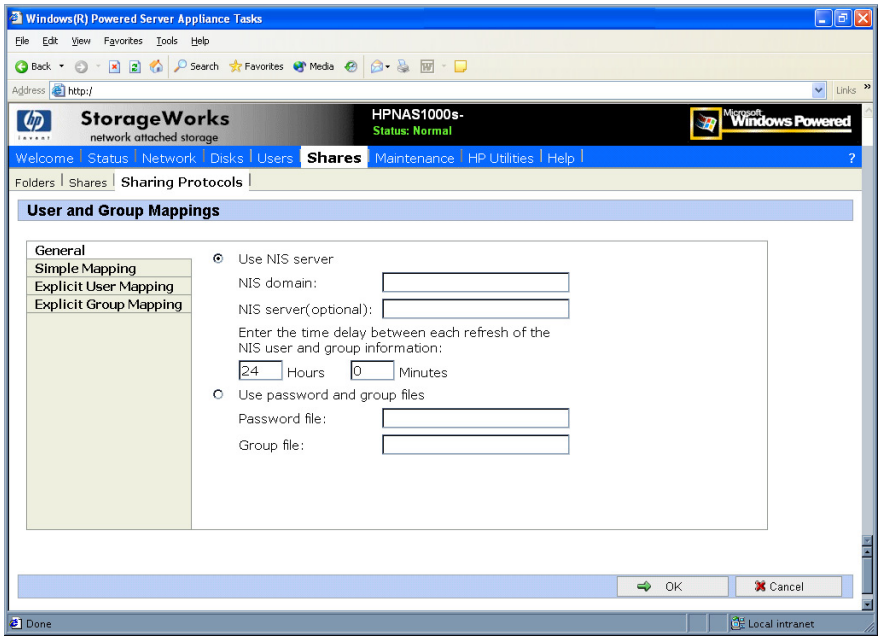

Figure 70: User and Group Mappings dialog box, General tab

From the **General** tab of the **User and Group Mappings** dialog box:

1. If an NIS server is being used:
   a. Select **Use NIS** server.
   b. Enter the NIS domain name.
   c. Enter the NIS server name. This field is optional. In the **Hours** and **Minutes** fields, indicate how often the system will connect to the NIS domain to update the user list.
2. If custom password and group files are being used:
   a. Select **User password and group files**.
   b. Enter the path and name of the password file.
   c. Enter the path and name of the group file.
3. After this basic information is entered, click **OK**.

Simple Mapping

Simple (or implicit) mapping is the first level of user name mapping. In simple mode, user and group names that match exactly in name are automatically equated.

While simple mappings are the most easily managed and are the most forthright type of map, security problems can arise. For example, if a UNIX user is coincidentally an exact match of a Windows user, the system will equate them and an inadvertent mapping will occur, granting a user inappropriate access.

To use simple mappings, the feature must be enabled. If this feature is turned off, the administrator must manually create an explicit map for each user.

To enable simple mapping, click the **Enable Simple Mapping** option and then select the Windows domain name.

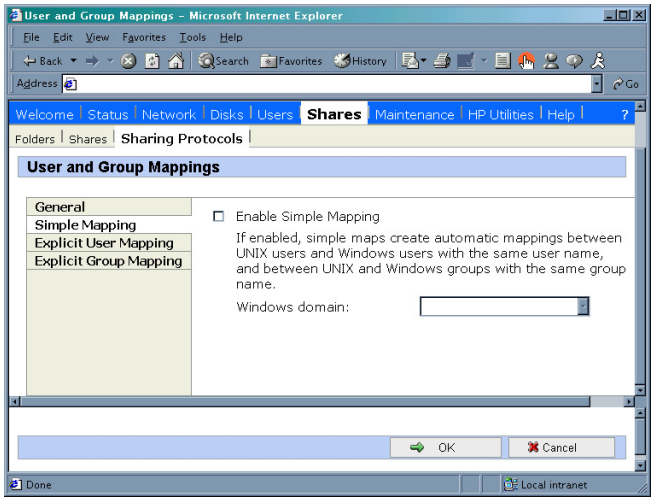
User and Group Mappings - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address
Go
Welcome Status Network Disks Users Shares Maintenance HP Utilities Help ?
Folders Shares Sharing Protocols
User and Group Mappings
General
Simple Mapping
Explicit User Mapping
Explicit Group Mapping
Enable Simple Mapping
If enabled, simple maps create automatic mappings between UNIX users and Windows users with the same user name, and between UNIX and Windows groups with the same group name.
Windows domain:
OK
Cancel
Done
Local intranet

Figure 71: User and Group Mappings dialog box, Simple Mapping tab

Explicit User Mapping

Explicit mappings allow the administrator to map any user or group manually to any other user and group. Advanced mappings override simple mappings, giving administrators the capability of using simple mapping for most users and then using advanced mappings for the users with unique names on the different systems. Alternatively, simple mapping can be disabled completely, relying solely on explicit mappings. Explicit mappings create the most secure mapping environment.

Security issues seen in simple mappings do not exist in explicit mappings. Explicit user mappings specifically correlate two users together, thus preventing the inadvertent mapping.

To enter explicit user mappings, select the **Explicit User Mapping** tab. Figure 72 is an example of the **Explicit User Mapping** tab.

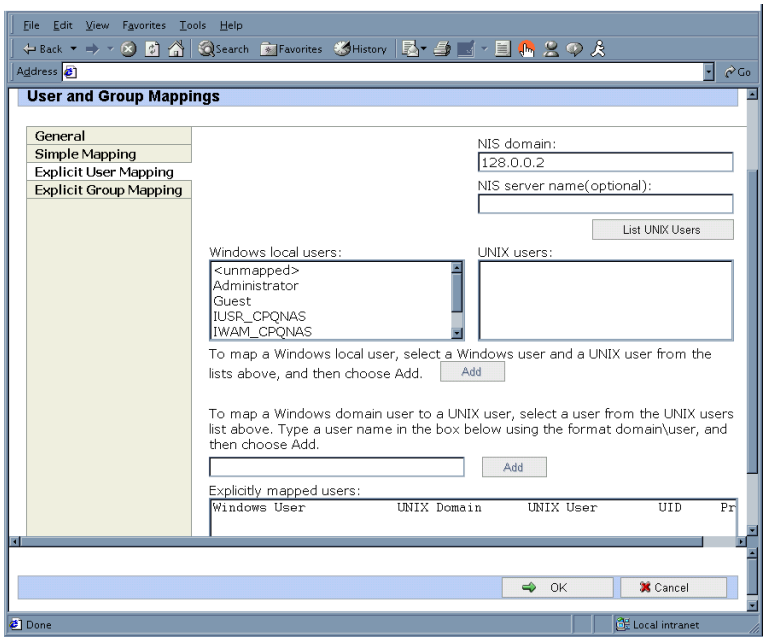

Figure 72: User and Group Mappings dialog box, Explicit User Mapping tab

To create explicit user mappings:

1. Click the **List UNIX Users** button to populate the UNIX users box.
2. To map a local Windows user to a UNIX user, highlight the **Windows user** in the Windows local users box and highlight the UNIX user that you want to map, and then click **Add**. The **Explicitly mapped users** box at the bottom of the screen is populated with the new mappings. Repeat this process until all desired users have been mapped.
3. To map a domain Windows user to a UNIX user, enter the domain and the user name in the box in the middle of the screen (use the Domain\username format) and highlight the UNIX user that you want to map, and then click **Add**. The map is added to the **Explicitly mapped users** box at the bottom of the screen. Repeat this process until all desired users have been mapped.
4. To map multiple Windows users to one UNIX user, one of the mapped Windows users must be set as the primary mapping. To indicate which user map is the primary mapping, highlight the desired map in the **Explicitly mapped users** box, and then click the **Set Primary** button.
5. To delete a map, highlight the map in the **Explicitly mapped users** box, and then click the **Remove** button.
6. After all entries are completed, click **OK** to activate the new entries.

Explicit Group Mapping

To enter explicit group mappings, select the Explicit Group Mapping tab. Figure 73 is an example of the **Explicit Group Mapping** tab.

Explicit mappings allow the administrator to map any user or group manually to any other user and group. Explicit mappings override simple mappings, giving administrators the capability of using simple mapping for most groups and then using explicit mappings to make changes to simple mappings. Simple mapping can be turned off for greater security.

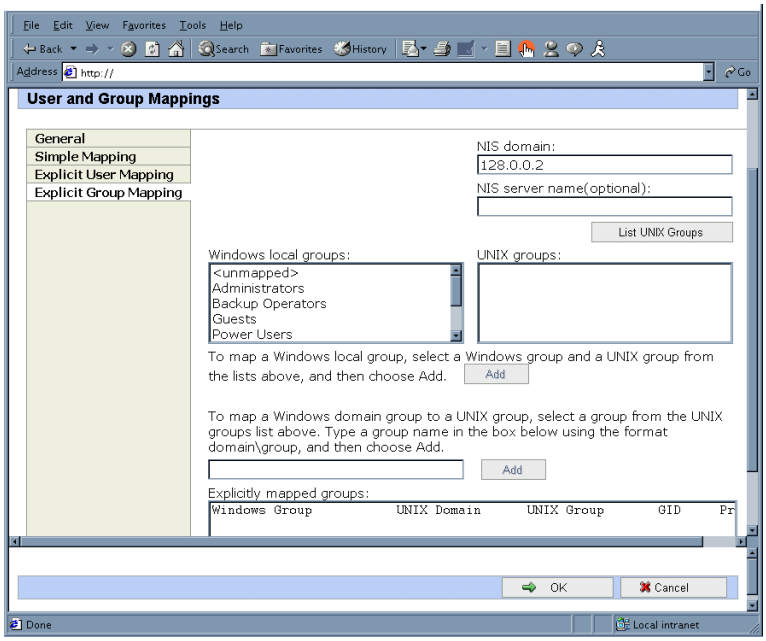

Figure 73: User and Group Mappings dialog box, Explicit Group Mapping tab

To create explicit group mappings:

1. Click the **List UNIX Groups** button to populate the **UNIX Groups** box.
2. To map a local Windows group to a UNIX group, highlight the Windows group in the Windows local groups box and highlight the UNIX group to map, and then click **Add**. The **Explicitly mapped groups** box at the bottom of the screen is populated with the new mappings. Repeat this process until all desired groups have been mapped.
3. To map a domain Windows group to a UNIX group, enter the domain and the group name in the box in the middle of the screen (use the Domain\groupname format) and highlight the UNIX group to map, and then click **Add**. The map is added to the **Explicitly mapped groups** box at the bottom of the screen. Repeat this process until all desired groups have been mapped.
4. To map multiple Windows groups to one UNIX group, one of the Windows groups must be set as the primary mapping. Therefore, to indicate which group map is the primary mapping, highlight the desired map in the **Explicitly mapped groups** box, and then click the **Set Primary** button.
5. To delete a map, highlight the map in the **Explicitly mapped groups** box and then click the **Remove** button.
6. After all entries are completed, click **OK** to activate the new entries.

Backing up and Restoring Mappings

The user name-mapping server has the capability to save and retrieve mappings from files. This capability is useful for backing up mapping settings prior to making changes and for exporting the mapping file from one server to others, using the same mapping information.

The user name-mapping server can save existing mappings to a file or load them from a file and populate the mapping server. This feature is found in the NAS Management Console under the **Map Maintenance** tab of the **User Name Mapping** screen, as shown in Figure 74.

To access the NAS Management Console, use Terminal Services. To open a Terminal Services session, from the WebUI, select **Maintenance**, **Terminal Services**.

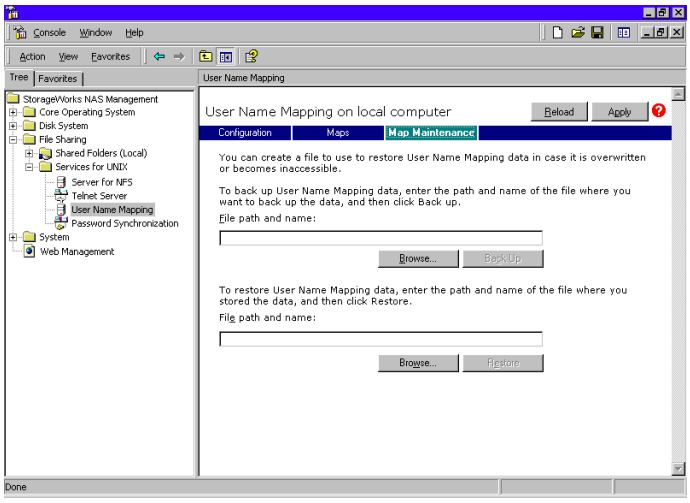

Figure 74: NAS Management Console User Name Mapping screen, Map Maintenance tab

Backing up User Mappings

1. Select the **Map Maintenance** tab from the **User Name Mapping** screen.
2. Type the path and name of the file to be used for backup in the File path and name field or click **Browse** to locate the file.

Note: If the file is being created for the first time, follow these steps:

---

1. Browse to the target directory.
2. Right-click in the file listing pane, select **New**, **Text Document**. Enter a name for the file and then press **Enter**.
3. Double-click the new file to select it.
4. Click **Backup**.

Restoring User Mappings

User mappings can be restored using the following procedures.

1. Select the **Map Maintenance** tab from the **User Name Mapping** screen.
2. Type the path and name of the file in the File path and name field or click **Browse** to locate the file.
3. After locating the file, click **Restore**.

NFS File Sharing Tests

HP recommends performing the following tests to verify that the setup of the shares, user mappings, and permissions grant the desired access to the NFS shares.

1. Create an NFS share.

   See "NFS File Shares" earlier in this chapter for information on creating shares.

2. Verify that the NFS share exists.

   Use Terminal Services to log in to the NAS 1000s and access the command line interface:

   `nfsshare <sharename>` (sharename represents the name of the share.)

3. Map a user.

   See "User and Group Mappings" in this chapter for instructions.

4. Verify that the mappings exist.

   Use Terminal Services to log in to the NAS 1000s and access the command line interface:

   `mapadmin list -all`

5. On the Linux/UNIX system, use the mapped user to create a file.

   a. As the root user, mount the share:

      `mount -t nfs <nfs server IP address:/nfs share> /mount point`

   b. Log in as a mapped user.

   c. Change directories to the mount-point directory.

   d. Create the file as the mapped user (example: *file1*).

6. Verify that the same permissions are set up for the user on both the UNIX side and the Windows side.

   a. List the permissions on the UNIX side:

      `ls -l /mount-point/file1`

      (Example screen display: -r--r----- unixuser1 unixgroup1)

   b. List the permissions on the Windows side: (change to the *nfs* share directory)

      From a command line interface accessed from Terminal Services on the NAS 1000s:

      `cacls file1`

      (Example display: DOMAIN1\Windowsuser1:R)

   c. Compare and verify the permissions from UNIX and Windows.

Terminal Services, Telnet Service, and Remote Shell Service

In addition to the WebUI, three services are available for remote administration of Services for UNIX. These services let users connect to machines, log on, and obtain command prompts remotely. See Table 4 for a list of commonly used commands.

Using Terminal Services

Microsoft Terminal Services can be used to remotely access the NAS 1000s Console. This provides the administrator flexibility to automate setups and other tasks. SFU file-exporting tasks and other SFU administrative tasks can be accomplished using Terminal Services to access the SFU user interface from the NAS Management Console or from a command prompt.

Terminal Services is included in the WebUI of the NAS 1000s. To open a Terminal Services session, from the WebUI, select Maintenance, Terminal Services. See the "Remote Access Methods and Monitoring" chapter for information on setting up and using Terminal Services.

Using Telnet Server

Telnet is a UNIX command line utility. The Telnet service is included on the NAS 1000s, but, by default, it is not activated. To use Telnet services, see the information in the "Remote Access Methods and Monitoring" chapter.

Using Remote Shell Service

The Remote Shell is a UNIX method for allowing UNIX users to run commands remotely. It can be used in a fashion similar to Telnet or can be used to directly invoke a remote command. Remote Shell service is not activated by default. See Chapter 11 for setup and use.

Table 4 describes some common SFU commands.

Table 4: Command Line Interface Command Prompts

Command	Function
`nfsstat /?`	Learn about viewing statistics by NFS operation type
`showmount /?`	View the format of the command to display NFS export settings on NFS servers
`showmount a`	View users who are connected and what they currently have mounted
`showmount e`	View exports from the server and their export permissions
`rpcinfo /?`	Learn how to display Remote Procedure Call (RPC) settings and statistics
`mapadmin /?`	View how to add, delete, or change user name mappings
`tnadmin /?`	View how to change Telnet Server settings
`nfsshare /?`	Learn how to display, add, and remove exported shares

Password Synchronization

Password synchronization is an optional service that automatically synchronizes Windows passwords with UNIX passwords across multiple machines or environments. This service is included on the NAS 1000s, but it is not activated.

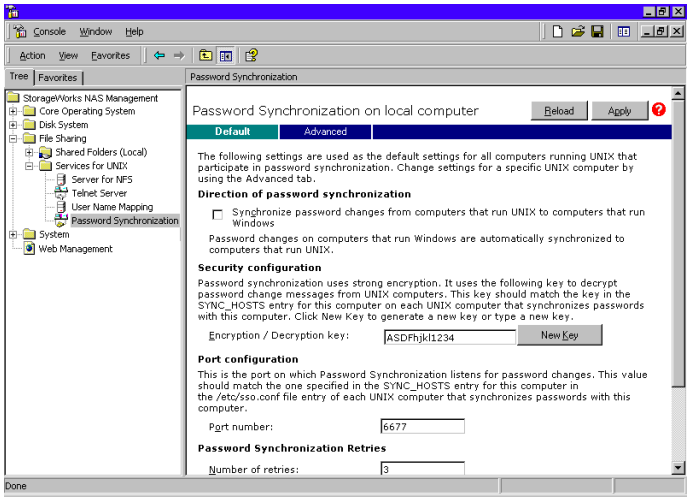
Console Window Help
Action View Favorites
Tree Favorites
Password Synchronization
StorageWorks NAS Management
Core Operating System
Disk System
File Sharing
Shared Folders (Local)
Services for UNIX
Server for NFS
Telnet Server
User Name Mapping
Password Synchronization
System
Web Management
Password Synchronization on local computer
Reload
Apply
Default
Advanced
The following settings are used as the default settings for all computers running UNIX that participate in password synchronization. Change settings for a specific UNIX computer by using the Advanced tab.
Direction of password synchronization
Synchronize password changes from computers that run UNIX to computers that run Windows
Password changes on computers that run Windows are automatically synchronized to computers that run UNIX.
Security configuration
Password synchronization uses strong encryption. It uses the following key to decrypt password change messages from UNIX computers. This key should match the key in the SYNC_HOSTS entry for this computer on each UNIX computer that synchronizes passwords with this computer. Click New Key to generate a new key or type a new key.
Encryption / Decryption key:
ASDFhjkl1234
New Key
Port configuration
This is the port on which Password Synchronization listens for password changes. This value should match the one specified in the SYNC_HOSTS entry for this computer in the /etc/sso.conf file entry of each UNIX computer that synchronizes passwords with this computer.
Port number:
6677
Password Synchronization Retries
Number of retries:
3
Done

Figure 75: Password Synchronization screen

Password synchronization ensures that the machines contain identical and most current user password database. When the user or administrator changes a password, the new password is updated across all target machines.

Without password synchronization, the user could have different passwords on different machines. If the administrator or user changed the password, the change would affect only that single machine.

Password Synchronization Best Practices

- Install Password Synchronization on all domain controllers to ensure consistent synchronization of the Domain and the UNIX passwords.
- Ensure consistent password policies.

  If you are providing Windows to UNIX password synchronization, make sure the Windows password policy is as restrictive in all areas as the UNIX policy. Failure to ensure that password policies are consistent may result in synchronization failure.
- Avoid synchronizing administrator passwords.

  Do not synchronize passwords for members of the Windows Administrator groups or the passwords of UNIX Superuser or Root accounts.

  — When Password Synchronization is installed, members of the local Administrators or Domain Administrators group are added to the PasswordPropDeny group, which prevents their passwords from being synchronized. If you add a user to either the Administrators or Domain Admins group, be sure to add the user to the PasswordPropDeny group.

  — The sync_users statement in the sso.conf file on UNIX systems prevents the passwords of Superusers from being synchronized.

Password Synchronization Requirements

For the password synchronization service to function, the work environment must meet the following criteria.

- The password policies must be the same on Windows NT and UNIX.
- User and group names must match exactly in spelling. No advanced mapping component exists to correct for any mistakes or differences.
- The UNIX system must be using CRYPT to encrypt its password database. If the UNIX machine is using anything else, such as MD5, the password synchronization service does not work.
- The password synchronization service must be installed on the primary and backup domain controllers. Click the Advanced button to select settings other than default.

Implementing Password Synchronization

The password synchronization service is a service residing on the NFS server. The service does not have to be on the same server as the NFS server, but the service is included on each NAS 1000s device. The password synchronization service detects updates on the Windows NT side and transmits the changes to the target UNIX machines, as specified in the service configuration.

To access the password synchronization module on the NAS device, use Terminal Services to access the **NAS Management Console**. From the **NAS Management Console**, select **File Sharing**, **Services for UNIX**, and **Password Synchronization**.

Configuring Advanced Settings

To configure advanced settings for password synchronization, use the following procedures:

1. Type the name or IP address of the UNIX computer in the **Computer Name** box.
2. Click **Add** and then click **Configure**. The password synchronization settings dialog box for the specific computer is displayed.

This dialog box allows the user to perform steps such as supplying new encryption keys or changing password synchronization port numbers.

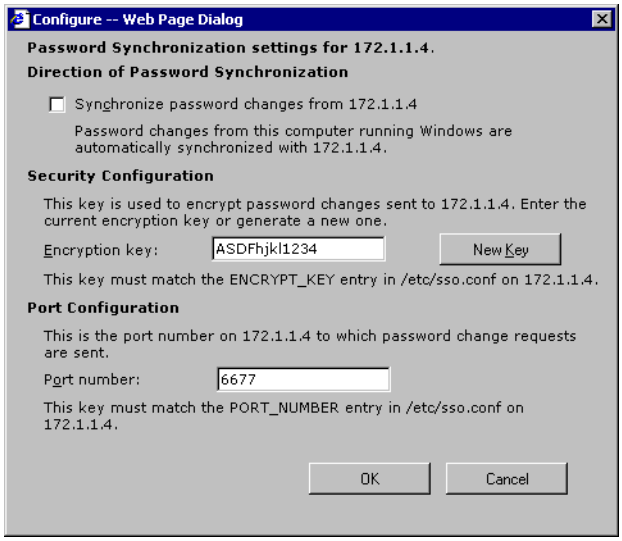
Configure -- Web Page Dialog
Password Synchronization settings for 172.1.1.4.
Direction of Password Synchronization
Synchronize password changes from 172.1.1.4
Password changes from this computer running Windows are automatically synchronized with 172.1.1.4.
Security Configuration
This key is used to encrypt password changes sent to 172.1.1.4. Enter the current encryption key or generate a new one.
Encryption key:
ASDFhjkl1234
New Key
This key must match the ENCRYPT_KEY entry in /etc/sso.conf on 172.1.1.4.
Port Configuration
This is the port number on 172.1.1.4 to which password change requests are sent.
Port number:
6677
This key must match the PORT_NUMBER entry in /etc/sso.conf on 172.1.1.4.
OK
Cancel

Figure 76: Password Synchronization screen, Advanced Settings dialog box

Installing Password Synchronization on Domain Controllers and Active Directory Domain Controllers

The password synchronization service must be installed on all primary domain controllers (PDCs) and backup domain controllers (BDCs) in a domain that will implement the password synchronization service. This includes Active Directory domains. The PDCs contain the primary copy of the user passwords.

Password synchronization should be installed by itself. Core SFU components are not needed to install the service on a domain controller.

Note: This procedure does not install SFU.

Caution: Before installing password synchronization, be sure to close all applications and notify connected users that the server is rebooting.

To install Password Synchronization without NFS Authentication Tools on a domain controller:

1. Allow the *C:\WINNT\bin\SFU* directory of the NAS 1000s to be shared:

   ```
   net share SFU=C:\WINNT\bin\SFU
   ```

2. On the domain controller, connect to the share:

   ```
   net use Z: \\NAS_machine_name\SFU
   ```

3. Change directories from the domain controller to the root of the connected share of the NAS 1000s:

   ```
   cd /d Z:\
   ```

4. Run the installation program on the domain controller (case sensitive):

```
OemSetup.msi ADDLOCAL=PasswdSync SFUDIR=C:\SFU
OEMINSTALL=TRUE SOURCELIST=Z:\ /l*v %temp%\sfusetup.log /q
```

5. Restart the domain controller. The domain controller must be restarted manually after installing the password synchronization. If the domain controller is not restarted, password synchronization will not run correctly.
6. Run the Administration User Interface on the domain controller and set up password synchronization:

   Click **Start**, **Programs**, **Windows Services for UNIX**, **Services for UNIX Administration**.

To install Password Synchronization and NFS Authentication Tools on the domain controller:

1. Allow the *C:\WINNT\bin\SFU* directory of the NAS 1000s to be shared:

   ```
   net share SFU=C:\WINNT\bin\SFU
   ```

2. On the domain controller, connect to the share:

   ```
   net use Z: \\NAS_machine_name\SFU
   ```

3. Change directories from the domain controller to the root of the connected share of the NAS 1000s:

   ```
   cd /d Z:\
   ```

4. Run the installation program on the domain controller in the following order (case sensitive):

   ```
   OemSetup.msi ADDLOCAL=NFSServerAuth SFUDIR=C:\SFU
   OEMINSTALL=TRUE SOURCELIST=Z:\ /l*v %temp%\sfusetup.log /q
   OemSetup.msi ADDLOCAL=PasswdSync SFUDIR=C:\SFU
   OEMINSTALL=TRUE SOURCELIST=Z:\ /l*v %temp%\sfusetup.log /q
   ```

5. Restart the domain controller. The domain controller must be restarted manually after installing the password synchronization. If the domain controller is not restarted, password synchronization will not run correctly.

Customizing Password Synchronization

Use Default to select password synchronization settings. Select different settings for each UNIX host in the Hosts tab.

- **Direction of Password Synchronization**—This option must remain unchecked. Password changes on Windows NT/2000 are always propagated to UNIX computers. Synchronize password changes from UNIX machines to Windows NT/2000.
- **Security configuration**—Password synchronization uses strong encryption for propagating passwords.
- **Encryption key**—Password synchronization comes with a default Encryption Key (displayed). Enter an encryption key of your own, regenerate the key, or do both.
- **Port configuration**—This port is where the password synchronization service checks for password changes. UNIX machines must be configured to use the defined port number.
- **Password Sync Retries**—Select **Password Sync Retries** to determine how Password Synchronization failures are handled.
- **Logging**—Significant password synchronization events are logged to the event log. Select the option to allow or deny extensive logging.

NetWare File System Management

7

File and Print Services for NetWare (FPNW) is one part of the Microsoft software package called Services for NetWare. The most common use of the NetWare network operating system is as a file and print server. Customers using NetWare as the platform to host their file and print services have become accustomed to its interface from both a user and an administrator point of view and have built up an investment in NetWare file and print services. File and Print Services for NetWare helps customers preserve their NetWare skill set while consolidating the number of platforms. This reduces hardware costs and simplifies file and print server administration by making the NAS 1000s emulate a NetWare file and print server. FPNW eases the addition of the NAS 1000s into a mixed infrastructure by providing a NetWare user interface (UI) to a Windows 2000-based server; administrators and users see their same, familiar NetWare UI. Additionally, the same logon for clients is maintained without a need for any client configuration changes.

This service also provides the ability to create Novell volumes, which are actually NTFS shares, from which users can map drives and access resources. Novell Login scripts are supported on the NAS 1000s or through an existing NDS (Novell Directory Services) account.

Note: IPX/SPX protocol is required on the Novell servers.

Topics discussed in this chapter include:

- Installing Services for NetWare
- Managing File and Print Services for NetWare
- Creating and Managing NetWare Users
- Managing NCP Volumes (Shares)

Installing Services for NetWare

The installation of FPNW on the NAS 1000s allows for a smooth integration with existing Novell servers. FPNW allows a Windows 2000-based server to emulate a NetWare file and print server to users, clients, and administrators. This emulation allows authentication from Novell clients, the use of Novel logon scripts, the creation of Novell volumes (shares), the use of Novell file attributes, and many other Novell features.

Additional information on Microsoft Directory Synchronization Services and the File Migration Utility can be found at:

www.microsoft.com/WINDOWS2000/guide/server/solutions/NetWare.asp

---

Note: The printing capabilities of File and Print Services for NetWare are not supported on the NAS 1000s.

To install Services for NetWare:

1. From the desktop of the NAS 1000s, click **Start**, navigate to **Settings-Network and Dial-up Connections**, click **Local Area Connection**, and then click **Properties**.
2. Click **Install**. The **Select Network Component Type** dialog box is displayed.

   Figure 77 is an example of the **Select Network Component Type** dialog box.

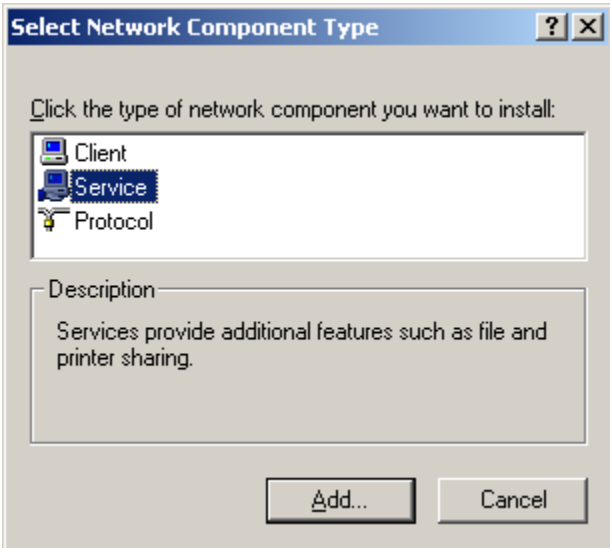

Figure 77: Local Area Connection Properties page, Install option

3. Select **Service** and click **Add**.
4. Click the **Have Disk** icon and navigate to the location of **Services for NetWare**.

   Services for NetWare is located in the path: *c:\hpnas\SFN\FPNW*.
5. Select the *NETSFNTSRV* file and click **OK**.

File and Print Services for NetWare should now appear as an option to install.

6. Select **File and Print Services for NetWare** and click **OK**.

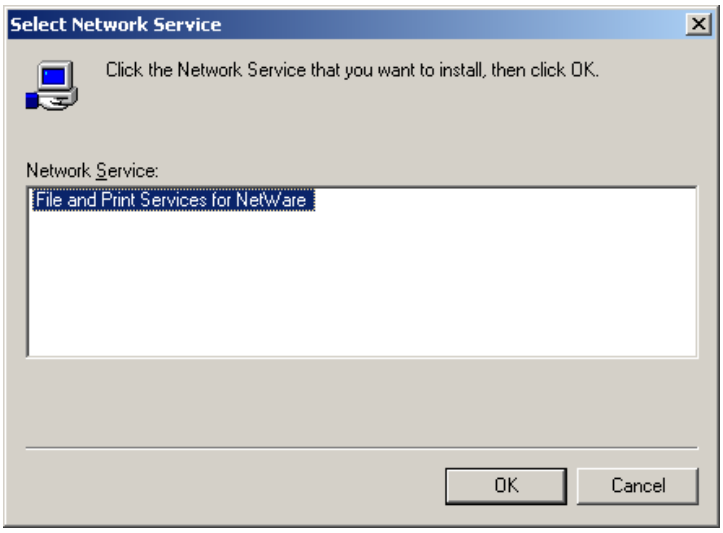
Select Network Service
Click the Network Service that you want to install, then click OK.
Network Service:
File and Print Services for NetWare
OK
Cancel

Figure 78: Installing File and Print Services for NetWare

Managing File and Print Services for NetWare

To access FPNW:

1. From the desktop of the NAS 1000s, click **Start**, **Settings**, **Control Panel**, and then double-click **FPNW**.

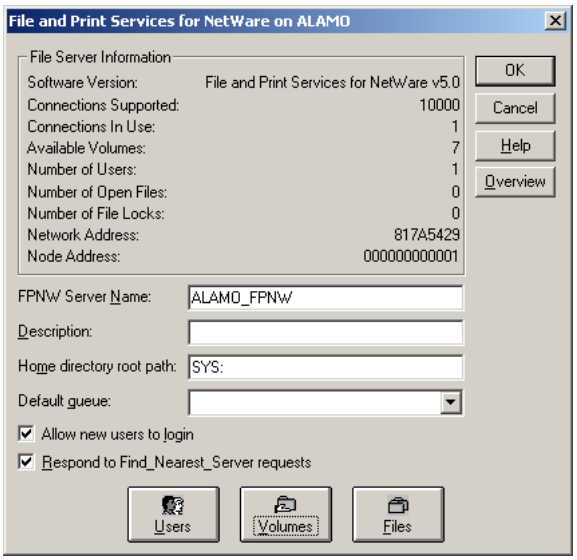

Figure 79: File and Print Services for NetWare screen

2. Enter an **FPNW Server Name** and **Description**.

   This name must be different from the server name used by Windows or LAN Manager-based clients to refer to the server. If you are changing an existing name, the new name will not be effective until you stop and restart **File and Print Services for NetWare**. For example, in Figure 79 the Windows server name is Alamo and the FPNW server name is Alamo_FPNW.

3. Indicate a **Home directory root path**.

   This path is relative to where the Sysvol volume has been installed. This will be the root location for the individual home directories. If the directory specified does not already exist, it must first be created.

4. Click **Users** to:

   See connected users, disconnect users, send broadcast messages to all users connected to the server, and to send a message to a specific user.

5. Click **Volumes** to:

   See users connected to specific volume and to disconnect users from a specific volume.

6. Click **Files** to:

   View open files and close open files.

Creating and Managing NetWare Users

To use Services for NetWare, the Novell clients must be entered as local users on the NAS 1000s.

Adding Local NetWare Users

1. From the NAS 1000s Console, click the **NAS Management Console** icon, click **Core Operating System**, and then click **Local Users and Groups**.
2. Right-click the **Users** folder and then click **New User**.

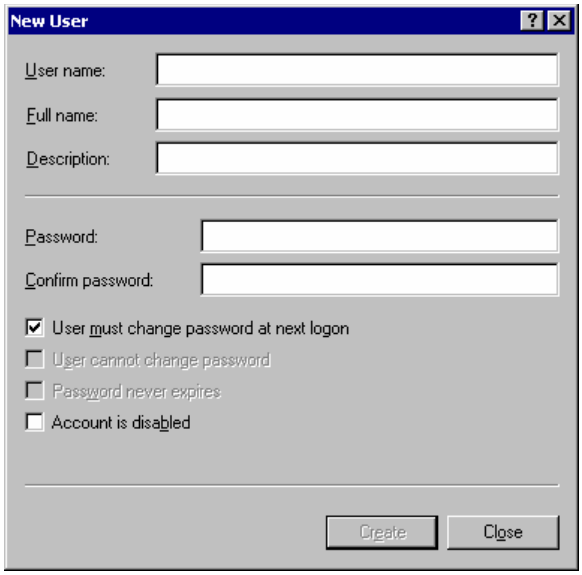

Figure 80: New User dialog box

3. Enter the user information, including the user's User name, Full name, Description, and Password. Click **Create**.
4. Repeat these steps until all NetWare users have been entered.

Enabling Local NetWare User Accounts

1. In the **Users** folder (NMC, Core Operating System, Local Users and Groups), right-click an NCP client listed in the right pane of the screen and then click **Properties**.
2. Select the **NetWare Services** tab.

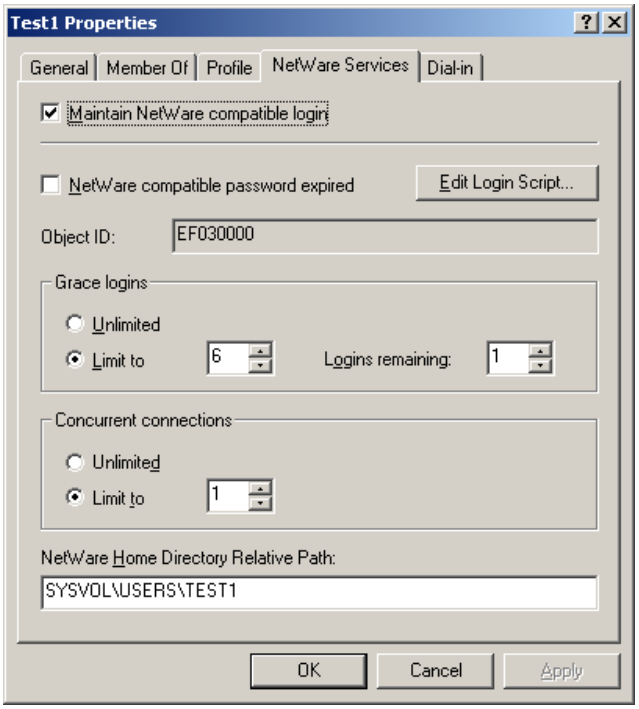

Figure 81: NetWare Services tab

3. Select **Maintain NetWare compatible login**.
4. Set other NetWare options for the user and click **OK**.

Note: The installation of File and Print Services for NetWare will also create a supervisor account, which is used to manage FPNW. The supervisor account is required if the NAS 1000s was added as a bindery object into NDS.

Managing NCP Volumes (Shares)

NCP file shares are created in the same manner as other file shares; however, there are some unique settings. NCP shares can be created and managed through two user interfaces:

- WebUI
- NAS Management Console

Procedural instructions for using each of these interfaces are included in the following sections.

Creating and Managing NCP File Shares Using the WebUI

Complete information on managing all types of file shares is documented in the "Shares Management" chapter of this guide. The following information is specific to NCP share management and is extracted from Chapter 5, Folder and Share Management, and duplicated below.

Note: NCP shares can be created only after Microsoft Services for NetWare is installed. See the previous section "Installing Services for NetWare" for instructions on installing SFN.

Shares can be managed through the Shares menu option of the WebUI. Tasks include:

- Creating a new NCP share
- Deleting an NCP share
- Modifying NCP share properties

Each of these tasks is discussed in this section.

Creating a New NCP Share

To create a new share:

1. From the WebUI main menu, select the **Shares** directory and then select the **Shares** option. The **Shares** dialog box is displayed. From the **Shares** dialog box, click **New**. The **General** tab of the **Create a New Share** dialog box is displayed.

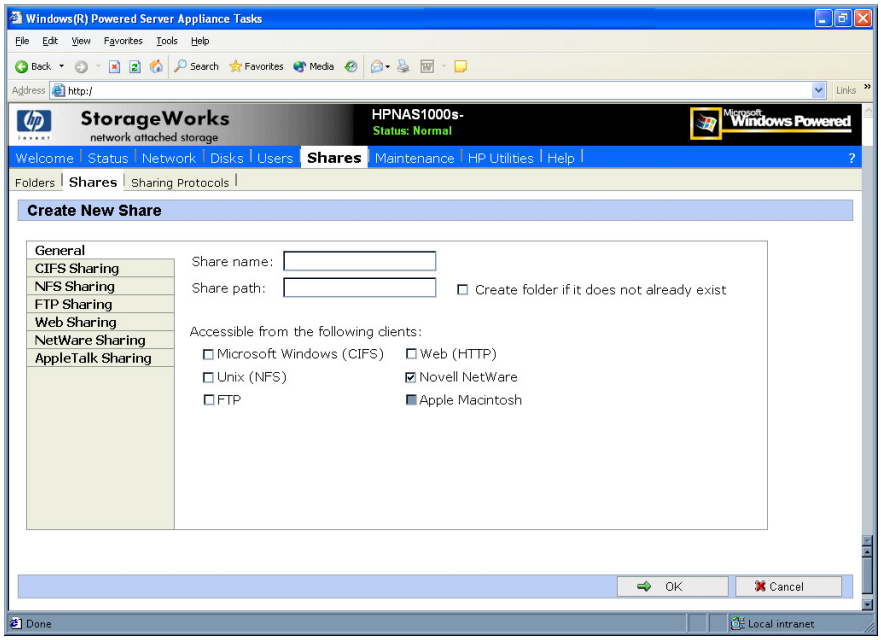

Figure 82: Create a New Share dialog box, General tab

2. In the **General** tab, enter the share name and path. Check the **Novell NetWare client protocol** checkbox.

   To create a folder for the share, check the indicated box and the system will create the folder when it creates the share.

3. Select the **NetWare Sharing** tab to enter NCP specific information. See "Modifying Share Properties" for information on this tab.
4. After all share information is entered, click **OK**.

Deleting an NCP Share

Caution: Before deleting a share, warn all users to exit that share. Then confirm that no one is using the share.

To delete a share:

1. From the **Shares** menu, click **Delete**.
2. Verify that this is the correct share and click **OK**.

Modifying NCP Share Properties

To change share settings:

1. From the **Shares** menu, select the share to modify and then click **Properties**. The **General** tab of the **Share Properties** dialog box is displayed.

   The name and path of the selected share are displayed.

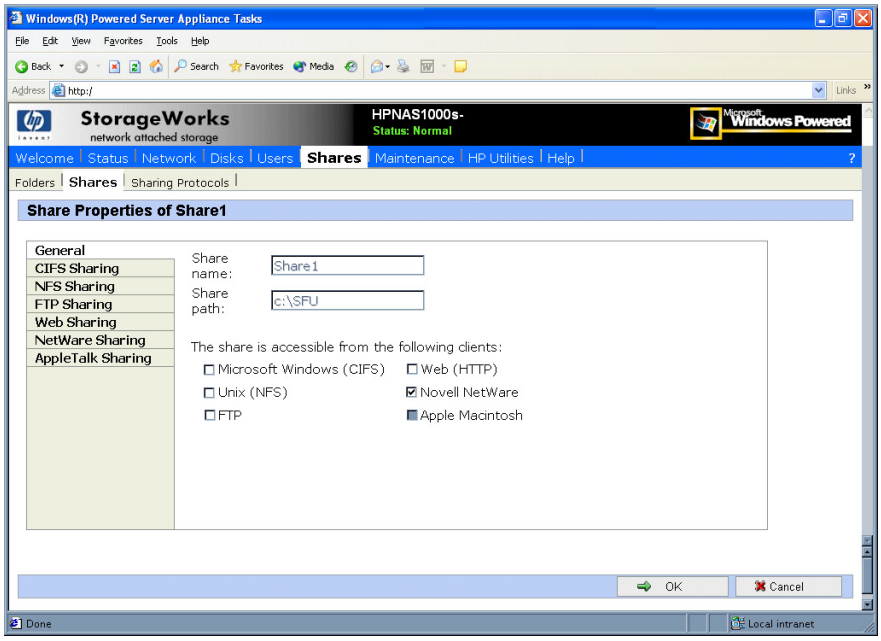

Figure 83: Share Properties dialog box, General tab

2. To enter or change client protocol information, check the **Novell NetWare client type** box and then click the **NetWare Sharing (NCP)** tab.

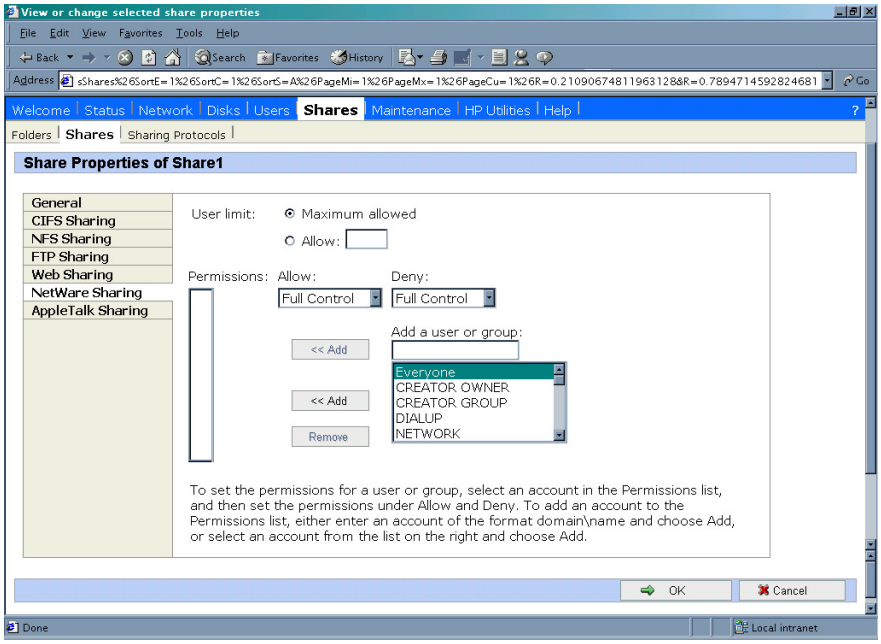

Figure 84: Share Properties dialog box, NetWare Sharing tab

3. From the **NetWare Sharing** tab of the **Share Properties** dialog box:
   a. Enter a user limit.
   b. Enter Permissions information.

      The **Permissions** box lists the currently approved users for this share.

      - *To add a new user or group*, either select a user or group from the box at the bottom right of the screen or manually enter the user or group name in the **Add a user or group** box. Then click **Add**. That user or group is added to the Permissions box.
      - *To remove access to a currently approved user or group*, select the user or group from the **Permissions** box, and then click **Remove**.
      - *To indicate the allowed access for each user*, select the user and then expand the **Allow** and **Deny** drop down boxes. Then, select the appropriate option.
4. After all NetWare Sharing information has been entered, click **OK**. The **Share** menu is redisplayed.

Creating and Managing NCP Shares using the NAS Management Console

In addition to the WebUI available on the NAS 1000s, shares can be managed through the NAS Management Console. Tasks include:

- Creating a new share
- Modifying share properties

Each of these tasks is discussed in this section.

Creating a New NCP Share using the NAS Management Console

To create a new file share:

1. From the NAS 1000s Console, click the **NAS Management Console** icon, click **File Sharing**, **Shared Folders**, and then **Shares**.
2. Right-click **Shares**, and then click **New File Share**. The **Create Shared Folder** dialog box is displayed.

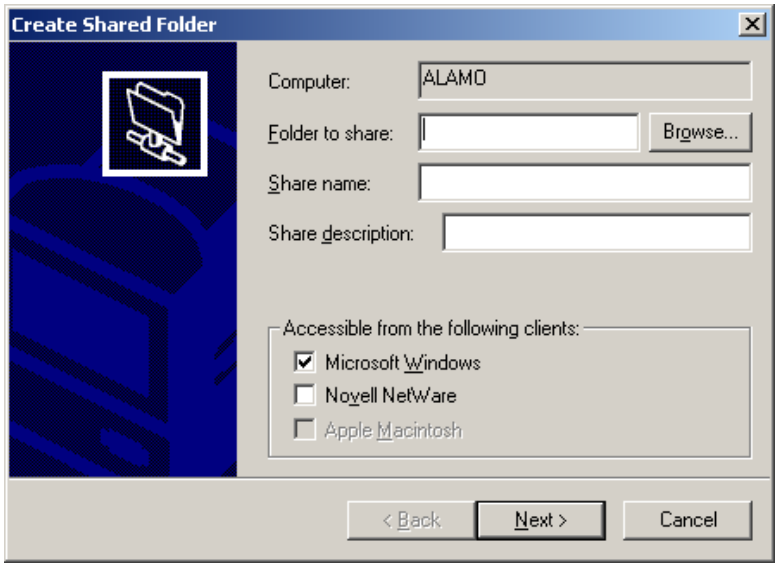

Figure 85: Create Shared Folder dialog box

3. In **Folder to Share**, type the path of the directory to be shared.
4. In **Share Name**, type the name of the share. Users will see this name.
5. In **Share Description**, type a description for the share.

6. Select the **Novell NetWare** checkbox and then click **Next**. The dialog box illustrated in Figure 86 is displayed.

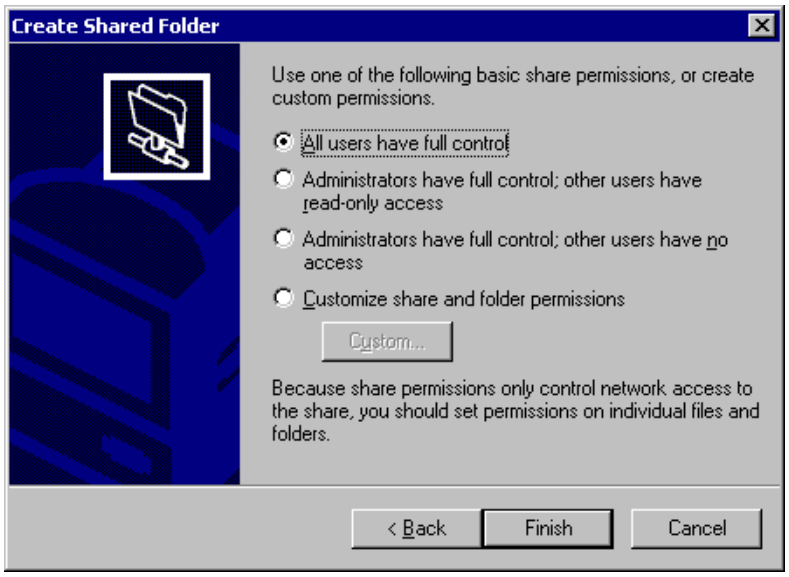
Create Shared Folder
Use one of the following basic share permissions, or create custom permissions.
All users have full control
Administrators have full control; other users have read-only access
Administrators have full control; other users have no access
Customize share and folder permissions
Custom...
Because share permissions only control network access to the share, you should set permissions on individual files and folders.
< Back
Finish
Cancel

Figure 86: NetWare Basic Share Permissions dialog box

7. Select the appropriate permissions level.

   If a custom permissions level is desired, select the **Customize share and folder permissions** radio button and then click **Custom**. The **Customize Permissions** dialog box is displayed. Figure 87 is an illustration of the **Customize Permissions** dialog box.

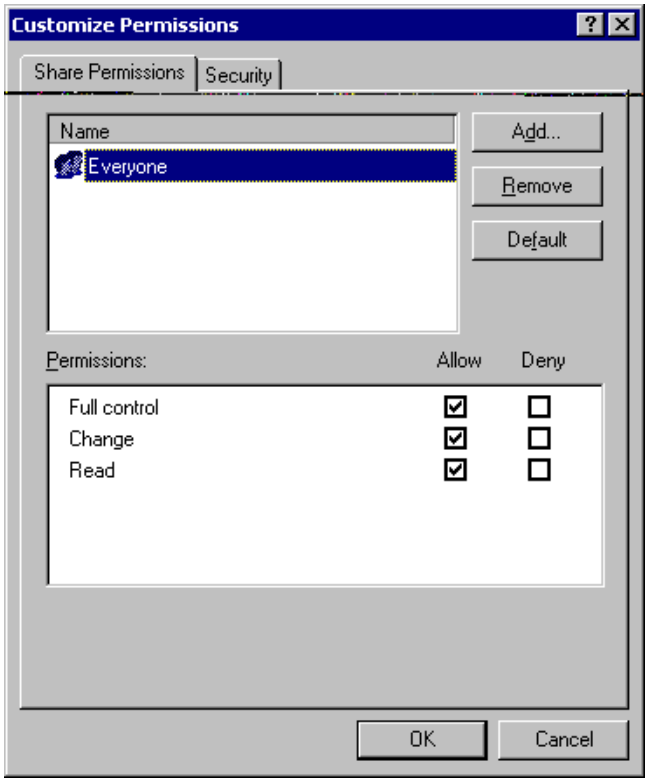

Figure 87: Customize Permissions dialog box, Share Permissions tab

8. In the **Share Permissions** tab, enter choose the appropriate permissions level for each user or group that is configured to have access to that share.
9. To enter file system permissions, select the **Security** tab. The following dialog box is displayed.

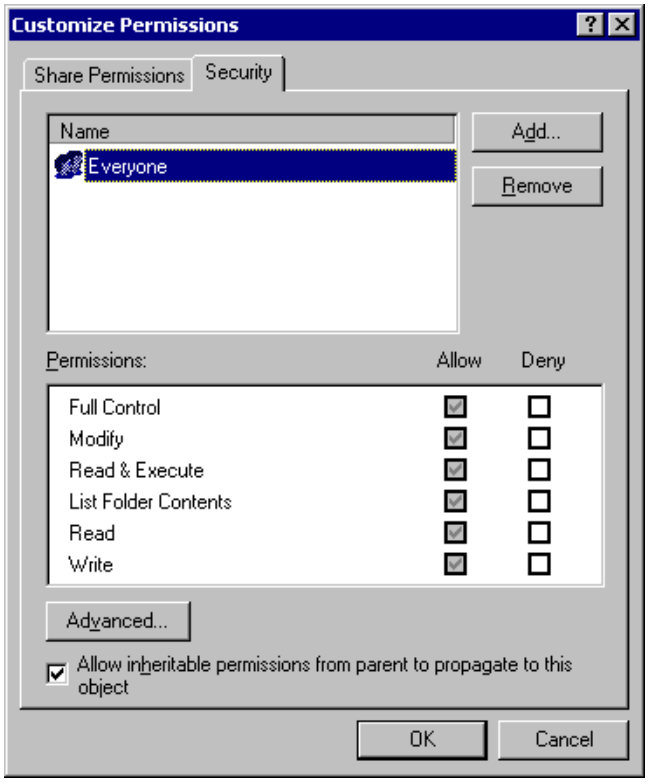

Figure 88: Customize Permissions dialog box, Security tab

10. In the **Security** tab of the **Permissions** dialog box, enter the file system security properties that apply to the share folder on the server.
11. After the permissions have been entered, click **OK** to return to the **Create Shared Folder** screens. Click **Finish** to create the share.
12. To create additional shares, click **Yes** at the "Create another shared folder" prompt. Otherwise, click **No** to exit.

Modifying NCP Share Properties using the NAS Management Console

To change share settings through the NAS Management Console:

1. From the NAS 1000s Console, select the **NAS Management Console** icon and then select **File Sharing**, **Shared Folders**, and **Shares**.
2. In the details pane, right-click the desired share and then click **Properties**.
3. Click the **Share Permissions** tab.
4. To grant permissions to an additional group or user, click **Add**, select the group or user, and then click **Add**. After any additional groups or users have been added, click **OK**.
5. To change the permissions granted to the group or user, select the desired group or user and then select **Allow** or **Deny** for each item.
6. To remove permissions for the group or user, select the desired group or user and them click **Remove**.

NOTES:

1. Permissions can be set on a shared volume regardless of its type of file system.
2. Share permissions are effective only when the share is accessed over the network.
3. The group of permissions you set for the share applies equally to all files and subdirectories in the volume.
4. Permissions on an NTFS share operate in addition to NTFS permissions set on the directory itself. Share permissions specify the maximum access allowed.

Remote Access Methods and Monitoring

8

The HP StorageWorks NAS 1000s comes from the factory with full remote manageability. Several methods of remote access are provided:

- Web based user interface
- Terminal services
- Telnet Server
  - — Enabling Telnet Server
  - — Configuring Telnet Server
- Remote Shell Daemon

These options let administrators use interfaces with which they are already familiar.

Web Based User Interface

The NAS 1000s includes a Web based user interface (WebUI) for the administrator to remotely manage the machine. Of all of the remote access methods, the WebUI is the most intuitive and easiest to learn and use.

The WebUI permits complete system management, including system configuration, user and group management, shares management, UNIX file system management, and storage management.

To access the WebUI:

1. Launch a Web browser.
2. In the URL field, enter:

   `http://<your NAS 1000s machine name or IP address>:3201/`

Extensive procedural online help is included in the WebUI.

Terminal Services

The NAS 1000s supports Terminal Services, with a license for two concurrently running open sessions. Terminal Services provides the same capabilities as being physically present at the server console.

Use Terminal Services to access:

- The NAS 1000s Console
- The NAS Management Console
- A command line interface
- Backup software
- Antivirus programs
- Telnet Server
- Remote Shell

To access Terminal Services from the WebUI, select Maintenance, Terminal Services. For additional procedural information on Terminal Services, see Chapter 2, Setup Completion and Basic Administrative Procedures

Telnet Server

Telnet Server is a utility that lets users connect to machines, log on, and obtain a command prompt remotely. Telnet Server is preinstalled on the NAS 1000s, but must be activated before use.

Caution: For security reasons, the Telnet Server must be restarted each time the server is restarted.

Enabling Telnet Server

To enable Telnet Server, use Terminal Services to access a command line interface and enter the following command:

```
net start tlntsvr
```

Configuring Telnet Server

To enter Telnet parameter settings, access the Telnet Server user interface. Use Terminal Services to go to the NAS Management Console. Then select **File Sharing**, **Services for UNIX**, **Telnet Server**.

In the Telnet Server UI, indicate the following:

- Authentication information
- Auditing information
- Server Settings
- Sessions information

Each of these topics is discussed in the following paragraphs.

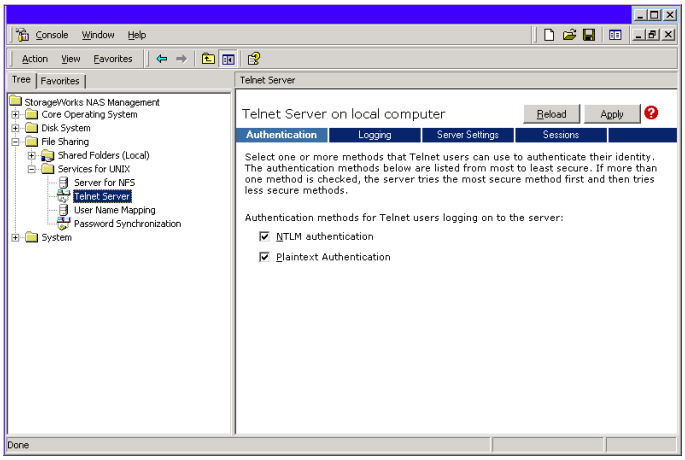

Figure 89: Telnet Server interface screen

Authentication Information

The **Authentication** tab is used to select user authentication methods allowed by the Telnet Server. The administrator determines what method of authentication is appropriate based on work environment.

Auditing Information

Telnet Server can log various events. The **Logging** tab allows the administrator to enable logging and select the events that should be logged. Note that errors and significant events are always logged to the Windows event list as well.

Server Settings

Use the **Server Settings** tab to change Telnet Server parameters. These parameters determine how the NAS 1000s Telnet Server operates. For example, one parameter is the number of simultaneous Telnet Server connections that the server allows.

Sessions Information

The sessions screen provides the ability to view or terminate active sessions.

Remote Shell Daemon

The remote shell, commonly referred to as rsh in UNIX, is a method for allowing users to access a command prompt or to run a command on another machine. It can be used in a fashion similar to Telnet Server or can be used to directly invoke a remote command.

Be default, the Remote Shell is not automatically started on the NAS 1000s. The administrator will need to start this service by entering the following command:

```
net start rshsvc
```

Note: For security reasons, each time the NAS 1000s is restarted, the Remote Shell service will have to be restarted.

In the following example, the remote shell runs the `ls -al` command on <server name> and returns the results to the screen:

```
rsh <server name> ls  al
```

Note: A .RHOSTS file must be created to allow client access to the server. See the SFU help topic "Rshsvc" on how to create the .RHOSTS file.

Currently, SFU implements only the remote command functionality of rsh. If a command line is needed, use Telnet Server.

For more information regarding the setup and use of Remote Shell or the Remote Shell service, refer to the online help documentation.

Backup Management

A

This appendix is a backup guide for HP StorageWorks NAS devices. This appendix guides the reader through the process of determining which backup and restore solution is best suited to the NAS device and their business environment.

As a source and a destination for departmental, workgroup, and enterprise data, the NAS 1000s becomes an integral part of company computing environments. Therefore, efficient backup and reliable restore capabilities are a priority.

This appendix provides pointers for setting up and maintaining reliable backups, including:

- Backup solutions
- Best practices

Backup Solutions

There are three main considerations when developing a backup solution:

- System environments
- Hardware options
- Software options

System Environments

In many departmental and workgroup situations, it is common to connect a tape backup device directly to the NAS device, using a SCSI connection. In this scenario, the server has exclusive use of the tape device. HP has several tape solutions with wide industry acceptance available for use with the NAS 1000s.

The NAS device is deployed into a SCSI direct connect environment.

SCSI Direct Connect Environments

The NAS device may be directly connected to a large tape library using an optional SCSI tape controller. The optional High Voltage Differential (HVD) or Low Voltage Differential (LVD) controllers have two SCSI busses, each capable of supporting up to two DLT 7000 (35/70 GB) devices, for a total of four tape drive devices.

Hardware Options

Selecting the correct type of device and connection ensures a reliable backup of data that is well suited to the particular computing environment. HP recommends several tape solutions for use with the NAS 1000s.

For a full list of qualified tape solutions, refer to the HP website:

www.hp.com

Additional backup recommendations and information is available in the Backup whitepapers, also available at the HP website.

Before purchasing a tape device, ensure that the backup software supports the preferred device. Most backup software supports a wide range of backup devices, and HP has done extensive testing and certification on many popular backup software packages. The administrator should confirm specific choices by consulting the software vendor's website. Vendors usually post a hardware compatibility guide for each version of the backup software application.

Software Options

After choosing the tape hardware devices, the next step is to select the backup software. If backup software is already being used on other servers, the same software may be used to reduce the complexity and setup time of the backup solution.

Before purchasing backup software, verify that it is supported on the chosen backup device. Most backup software supports all types of backup devices, and HP has done extensive testing and certification on many popular backup packages. The administrator must confirm the specific choice by consulting the software vendor's website. Vendors usually post a hardware compatibility guide for each version of the backup software application.

Important capabilities to look for in backup software include the following:

- Autochanger support
- Tape media management database
- File history database with extensive search capabilities
- Ability to define backup groups and schedules
- Ability to take advantage of multiple tape devices concurrently, to reduce backup window
- Capabilities to analyze, summarize, and report status automatically
- Options for sharing tape drives in a shared library environment
- Options to enable backup of open and locked files
- Options to back up system state and system databases
- Options to interact with software from a remote console application
- Options for disaster recovery

Best Practices

After deciding on a backup solution, establish procedures that will enhance the reliability and effectiveness of the backups. The following sections describe general recommendations for performing a backup. Keep company specific needs and environment in mind when implementing these suggestions.

Regular and Reliable Backups

The NAS 1000s uses RAID 5 for data protection and high availability. The RAID 5 configuration is not user configurable. This configuration makes data loss due to disk failure unlikely, because two drives in the same array must fail at the same time for data loss to occur. Although unlikely, such a failure can occur. Despite this feature, the only way to reliably safeguard data against accidental loss, intentional tampering, or hardware failures is with regularly scheduled backup and offsite storage of backup media. Backups prevent an inconvenience from becoming a tragedy.

Automated Tape Libraries

Automated tape libraries improve performance, capacity, and reliability of tape backup operations and should be used whenever possible. Libraries must be enabled by additional licensing, installation of library control modules, and configuration steps. Benefits of tape libraries include:

- Enhanced performance by the automated, instantaneous handling of tapes, requiring no lag time for an administrator to arrive and manually change the tape.
- Improved capacity because tape libraries include storage slots for additional tape cartridges. Enough media can be loaded so that operations can continue overnight, over the weekend, or all week, without intervention or tape changes.
- Increased reliability because tapes are handled less and the human element of forgetfulness in changing tapes is eliminated.

Multiple Backup Devices

To take advantage of multiple backup devices, the server must be configured correctly. Generally, backing up multiple disks requires multiple tape drives. If the NAS device has 500 GB of disk space and this space is arranged as a single volume, it is not possible to directly take advantage of multiple tape drives. If possible, make multiple, smaller volumes. This procedure lets the administrator back up the multiple devices in parallel, sending the data from one or two disks to each tape in parallel. This type of configuration greatly reduces the time required for backup and makes the most efficient use of the tape backup device.

If it is necessary to use a single volume, the administrator configures several backup groups to contain the various directory trees at the root, so that more than one tape device can work in parallel.

Also, note how the volumes are constructed when setting up backup jobs. To increase the performance of the backups, schedule the back up of volumes so that disks that share a common set of physical drives are scheduled at different times. The underlying physical disks can devote more time to each of the backup jobs, rather than having two backup jobs competing for disk I/O.

Backup Schedules

An automatic, periodic backup is much more reliable than occasional backups that occur only when someone remembers to execute them. The specific needs of the organization will determine what type of schedule to implement.

A weekly or biweekly full backup is the basis of any good backup schedule. Add to that baseline daily incremental or differential backups to capture any daily changes that occur between full backups. Depending on the rate of data change, and the capacity and performance of the backup devices, adjust the backup schedule to fit the environment of the organization. Incremental backups capture changes to the data that have occurred since the last backup. Differential backups capture all the changes that have occurred since the last full backup.

If the backup devices do not have sufficient capacity for a complete, full backup, distribute the backups so they occur throughout the backup cycle. This strategy can meet the backup needs of the organization until a larger tape backup device or library can be installed. For example, instead of doing a full backup of disks C:, X:, Y:, and Z: on Friday, back up C: on Monday, X: on Tuesday, Y: on Wednesday, and Z: on Thursday. Schedule incremental or differential backups on the same distributed schedule.

Note: The suggested scenarios for backup times are based on a hypothetical company situation.

Media Rotation

Most backup software solutions are equipped to label and track media usage accurately. Take advantage of these capabilities to maintain different media pools for full backups and incremental/differential backups, as well as archive media. The retention time on each of these types of backup is different. For example, using differential backups on the same tape as for full backups causes the tape space to be wasted after the retention time for the differential data has passed. Keep separate pools to avoid this problem.

Offsite Storage

Set up a regular process for moving important long term media, such as backups and archives, offsite for safekeeping. This ensures that the administrator can recover the data in the event of a complete facility destruction where the NAS device resides. As an alternative to a commercial offsite storage facility, if the company has multiple buildings, the offsite media can be stored in another building. This alternative provides some protection in the event of a building fire where the NAS device is located.

When employing offsite storage, strike a balance between safety and convenience by deciding how long to keep the media onsite. After the media has been moved offsite, restores will take much longer because the media is not readily available.

A periodic audit of the offsite facility ensures the media is being stored in secure, environmentally acceptable conditions, and that it can be located and returned to the facility in a timely manner.

Server Setup Information Archival

After the administrator has established a regular backup schedule, it is necessary to document the setup attributes of the NAS device. To maximize the ability to recover from server disasters and to minimize the time required for recovery, keep current copies of the following information in a safe location:

- Server name
- IP addresses
- Gateways
- DNS servers
- NIS servers
- User mapping database
- Storage setup
  - Member storage units (LUNs)
  - Share names, paths, and access permission settings

This information greatly increases the ability to quickly and accurately recover from catastrophic failures such as fires, weather disasters, theft, and complete hardware failure.

Snapshots and Quick Online Restores

Persistent Storage Manager (PSM) provides instant data recovery from hundreds of online snapshots. Once the first snapshot is taken PSM monitors all drive activity retaining the deleted data required to recreate the last snapshot. Individual files, groups of files, folders, groups of folders or complete volumes can be restored. Security rights and privileges, as well as file and directory attributes, remain in effect as they were at the time the snapshot was created.

Snapshots can be used as a convenient source of data for a backup. There are some applications that must be stopped before backups are made. A backup requires that the file system is recorded in a consistent state, where no changes occur during the backup. Because snapshots are created in a matter of seconds and maintain a consistent view of the file system from that point on, snapshots can drastically reduce the amount of time applications must be paused or shut down during backup operations. The NAS device facilitates automatically creating snapshots at any given time.

Caution: Snapshots should be considered an additional convenience for restores, not a replacement for tape backup. In the event of disk failures, snapshots can be lost along with the original data. Snapshots will be automatically deleted without warning by PSM to regain space when disk space is low.

Although snapshots should never be considered a replacement for regular data backup to removable media, they can be a highly convenient feature for immediate, tapeless recoveries. If a file is accidentally deleted or corrupted, it can be recovered quickly by accessing the snapshot, selecting the file or directory, and copying it back to its original location on the volume.

To use the snapshot capability for a quick online restore, take a snapshot on a regular basis or before the source disk is altered. This ensures a backup of all the original files, applications, and configurations.

Readiness Testing

Completing regular backups is important, but it is only the first step in the backup process. To verify the integrity of those backups, the administrator must conduct periodic testing to confirm the ability to recover files and directories. Regularly testing the recoverability of random files or directories ensures that the backup solution is working as planned.

Disaster Recovery

Disasters that cause the loss of an entire server or server operating system drives require a complete restoration of the server. The specific procedure for recovering from a disaster depends on your environment, the backup software, and the optional disaster recovery modules that may have been installed.

In general, it is necessary to complete the following steps to fully recover from a disaster:

- Power up the server using the secondary boot partition.
- Backup the data using the installed backup application.
- Use the QuickRestore process to reinstall the NAS 1000s system image.

Caution: Performing a QuickRestore process will destroy all data on the server. Make sure to perform a backup of the data before performing a QuickRestore.

- Reinstall the backup application.
- Add the NAS 1000s into the appropriate domain.
- Re-establish user accounts if the NAS 1000s is a part of a workgroup.

  If the files were retained, re-establish user rights to drives, files, and directories.

Note: Being a part of a domain negates this requirement.

- Recover the backup application file and media history databases.
- Recover data from backup applications.
- Recover the system state.
- Re-create file shares.

PSM Error Codes

B

If you experience a problem using Persistent Storage Manager, the following list of event log messages can be used to troubleshoot. Error codes are logged to the system event log by the file system driver for Persistent Storage Manager, PSMAN5 driver; each entry appears with "psman5" as the source name.

Table 5: PSM Error Codes

Error Code	Description
0x00000001	An invalid IOCTL was sent to the driver. Action: Save the system eventlog and contact technical support
0x00000002	Device name is not recognized by PSM. Action: Save the system eventlog and contact technical support.
0x00000003	An invalid path was given for the cache file. Explanation: This error will appear if the cache file cannot be created because the cache file drive is not present. Action: Save the system eventlog, contact technical support.
0x00000005	An exception occurred. Action: Save the system eventlog, contact technical support.
0x00000005	You do not have sufficient rights to the cache file directory. Action: Make sure you have full access to the cache file directory
0x00000005	The cache file specified is a directory instead of a file. Action: Give a full path and filename for the cache file.
0x00000005	PSM was told to shut down. Action: Save the system eventlog and contact technical support.
0x00000006	User performing PSM function without opening PSM. Action: Programmatically, PSM must be opened before a command can be submitted.
0x00000015	Access to a virtual volume has been attempted after it has been destroyed. Action: Do not access virtual volumes after they have been destroyed.
0x00000016	Something has gone wrong with PSM. Action: Save the system eventlog and contact technical support.
0x00000017	Bad sector was detected in the cache file. Action: Save the system eventlog and contact technical support.
0x0000001F	General failure. Action: Save the system eventlog and contact technical support.

Table 5: PSM Error Codes

Error Code	Description
0x00000057	An invalid parameter was passed to a function. Action: Programmatically, verify the parameters being passed to PSM are correct.
0x00000079	I/O timed out while reading from the cache file. Action: Verify the hard drive is operational.
0x0000007A	Buffer size supplied is insufficient to hold requested information. Action: Save the system eventlog and contact technical support.
0x000000A1	An invalid path was given for the cache file. Action: Save the system eventlog and contact technical support.
0x000000EA	Buffer size supplied is insufficient to hold requested information. Action: Save the system eventlog and contact technical support.
0x000003E6	An exception occurred. Action: Save the system eventlog and contact technical support.
0x00000456	PSM was stopped because the media of a device being PSM'ed was changed. Action: You can take a new snapshot now
0x0000045D	An error occurred on the device. Action: Save the system eventlog and contact technical support.
0x000005AA	There is insufficient memory available. Action: Close unnecessary applications or add more memory.
0x000006F8	Buffer size supplied is insufficient to hold requested information. Action: Save the system eventlog and contact technical support.
0x000006F8	Invalid buffer address passed for I/O. Action: Save the system eventlog and contact technical support.
0x80000005	Specified buffer size is too low. Action: Save the system eventlog and contact technical support.
0x8000001C	PSM was stopped because the media of a device being PSM'ed was changed. Action: Take a new snapshot.
0xA0000004	The cache file is <x>% full. The oldest snapshot(s) will automatically be deleted at <y>%. Explanation: This is a warning that the cache file size is approaching the threshold at which some snapshots will be deleted automatically to free up some cache file capacity. <x> is the percentage for which the warning message will be generated, and <y> is the percentage which represents the threshold. (By default, these values are 80% and 90%, respectively, and can be modified in Windows 2000 for NAS (Disks/Persistent Storage Manager).) Action: In Windows 2000 for NAS (Disks/Persistent Storage Manager)), delete some (non-critical) snapshots before the system does to guarantee that critical snapshots do not get deleted accidentally.
0xC0000001	General failure. Action: Save the system eventlog and contact technical support.
0xC0000002	Function is not yet implemented. Action: Save the system eventlog and contact technical support.

Table 5: PSM Error Codes

Error Code	Description
0xC0000005	An Access Exception occurred. Action: Save the system eventlog and contact your vendor's technical support.
0xC0000008	User performing PSM function without opening PSM. Action: Save the system eventlog and contact technical support.
0xC000000D	An invalid parameter was passed to a function. Action: Save the system eventlog and contact technical support.
0xC000000E	Device name is not recognized by PSM. Action: Save the system eventlog and contact technical support.
0xC0000010	An invalid IOCTL was sent to the driver. Action: Save the system eventlog and contact technical support.
0xC0000013	Access to a virtual volume has been attempted after it has been destroyed. Action: Do not access virtual volumes after they have been destroyed.
0xC000001C	An invalid IOCTL was sent to the driver. Action: Save the system eventlog and contact technical support.
0xC0000022	An access exception occurred. Action: Save the system eventlog and contact technical support.
0xC0000022	You do not have sufficient rights to the cache file directory. Action: Save the system eventlog and contact technical support.
0xC0000023	Specified buffer size is too small. Action: Save the system eventlog and contact technical support.
0xC0000034	Cache file name is invalid. Action: Save the system eventlog and contact technical support.
0xC000003A	An invalid path was given for the cache file. Action: Save the system eventlog and contact technical support.
0xC000003B	An invalid path was given for the cache file. Action: Save the system eventlog and contact technical support.
0xC000003E	Bad sector was detected in the cache file. Action: Save the system eventlog and contact technical support.
0xC0000043	A file cannot be opened because the share access flags are incompatible. Action: This occurs when the very last snapshot is deleted. PSM initializes its files when the last snapshot is deleted. While it is initializing, a new snapshots can not be created. Try again in a few minutes.
0xC000009A	There is insufficient memory available. Action: Save the system eventlog and contact technical support.
0xC00000B5	I/O timed out while reading from the cache file. Action: Save the system eventlog and contact technical support.
0xC00000BA	The cache location must be a file rather than a directory. Action: Save the system eventlog and contact technical support.
0xC00000E8	Invalid buffer address passed for I/O. Action: Save the system eventlog and contact technical support.

Table 5: PSM Error Codes

Error Code	Description
0xC000010A	PSM was told to shut down. Action: Save the system eventlog and contact technical support.
0xC0000184	Something has gone wrong with PSM. Action: Save the system eventlog and contact technical support.
0xC0000185	An error occurred on the device. Action: Save the system eventlog and contact technical support.
0xC0000206	Buffer size supplied is insufficient to hold requested information. Action: Save the system eventlog and contact technical support.
0xE0001001	PSM could not start due to the server being constantly busy for minutes. Action: Take a snapshot when the system demands are lower.
0xE0001002	PSM detected a deadlock. Action: Check what other filter drivers you are running (i.e., virus scanners, etc.) Save the system eventlog and contact technical support.
0xE0001003	Specified volume not active or deleted. Action: Do not delete volumes with active snapshots.
0xE0001004	PSM was specified for a volume that is currently not being PSM'ed. Action: Save the system eventlog and contact technical support.
0xE0001005	Cache file overflow caused all existing snapshots to be deleted. Action: Increase the cache file size in Windows 2000 for NAS (Disks/Persistent Storage Manager), or take/schedule snapshots when fewer users are online.
0xE0001006	The application tried to enable PSM without first calling Psm_Register. Action: Programmatically, a program must register with PSM prior to sending it commands.
0xE0001007	Invalid license code. Action: Contact vendor for a valid license.
0xE0001008	Another application already has PSMed locked exclusively. Action: Save the system eventlog and contact technical support.
0xE0001009	PSM needs to be locked exclusive for this function to work. Action: Save the system eventlog and contact technical support.
0xE000100A	Wrong version of the driver has been loaded on this system. Action: Verify the PSM version, save the system eventlog and contact technical support.
0xE000100B	A reboot is required before PSM can operate. Action: Reboot the machine, and try taking a snapshot again. If this still fails, save the system eventlog and contact technical support.
0xE000100C	PSM is not installed. Action: Save the system eventlog and contact technical support.
0xE000100D	An incompatible DLL from another version of PSM is already loaded. Action: Verify the PSM version, save the system eventlog and contact technical support.
0xE000100E	Out of memory. Action: Close unnecessary applications or add more memory.

Table 5: PSM Error Codes

Error Code	Description
0xE000100F	Invalid parameter. Action: Save the system eventlog and contact technical support.
0xE0001010	Invalid handle. Action: Save the system eventlog and contact technical support.
0xE0001011	Not implemented yet. Action: Save the system eventlog and contact technical support.
0xE0001012	Object type is not expected object. Action: Save the system eventlog and contact technical support.
0xE0001013	User buffer is not large enough. Action: Save the system eventlog and contact technical support.
0xE0001014	Out of available structures. Action: In Windows 2000 for NAS (Disks/Persistent Storage Manager), delete some snapshots.
0xE0001015	PSM is shutting down. Action: This is not an error but is a status message.
0xE0001016	The device, volume or object does not exist. Action: Verify that the device, volume, or object exists.
0xE0001017	Unsuccessful. Action: Save the system eventlog and contact technical support.
0xE0001018	The device does not have any media loaded. Action: If the snapshot has been deleted, it cannot be accessed
0xE0001019	Object already exists. Action: Save the system eventlog and contact technical support.
0xE000101A	Specified path is a directory and not a file. Action: Provide a full path and filename
0xE000101B	Invalid path was specified. Action: Ensure the CacheFile name is correct
0xE000101C	The static volume was not mounted. Action: Look at the system event log for a warning message (from the PSMAN5 service) whose code should appear this list. The action depends on the message.
0xE000101D	The static volume had errors during mount. Action: Look at the system event log for a warning message (from the PSMAN5 service) whose code should appear in this list. The action depends on the message.
0xE000101E	The static volume could not be found. Action: Save the system eventlog and contact technical support.
0xE000101F	The volume the cache file resides on is out of space. Action: The cache file for each volume resides on the volume itself. Free some space on the volume.
0xE0001020	The volume the cache file resides on was dismounted. Action: The cache file for each volume resides on the volume itself. Do not dismount the volume.

Table 5: PSM Error Codes

Error Code	Description
0xE0001021	The server was shutdown. Action: Do not shut down the machine while snapshots are in progress.
0xE0001022	Unable to create cache file. Action: Save the sysktem eventlog and contact support.
0xE0001023	PSM recovery could not find a snapshot entry. Explanation: A snapshot was lost during the recovery process. It is unknown which snapshot it was. Action: Save the system eventlog and contact technical support.
0xE0001024	PSM recovery could not open the index file. Explanation: All snapshots are corrupt. Action: Save the system eventlog and contact technical support.
0xE0001025	PSM recovery encountered error <x> inserting key (<y>:<z>) into dictionary. Explanation: <x> is the error that occurred and can be found in this list of errors. Action: Look up the error in this list and take the specified action.
0xE0001026	PSM recovery encountered corrupt index sector %2. Explanation: An index entry was found to be corrupt during the last boot. Action: Save the system eventlog and contact technical support.
0xE0001027	A snapshot could not be created due to error 0x<x>. Explanation: <x> is the error that occurred. Action: Look up the error in this list and take the specified action.
0xE0001028	The cache file is <x>% full. Snapshots have been deleted. Explanation: The oldest snapshots have been deleted. Action: In Windows 2000 for NAS (Disks/Persistent Storage Manager), delete snapshots to make sure specific (critical) snapshots are not destroyed by mistake.
0xE0001029	The maximum (<x>) allowed snapshots has been reached. A snapshot was not created. Explanation: PSM cannot create any more snapshots because the configured maximum number of snapshots that PSM can keep concurrently has been reached. Action: In Windows 2000 for NAS (Disks/Persistent Storage Manager) increase the number of snapshots allowed, or edit the schedules to not make so many snapshots.
0xE000102A	The evaluation period has expired. Action: Contact your vendor's technical support for a non-evaluation version.
0xE000102B	There is not enough free cache space to perform the operation. Action: Delete some snapshots to free up some cache space of enlarge the cache file.
0xE000102D	The maximum number of snapshots has been reached. The oldest snapshot was deleted to allow creation of a new snapshot. Action: Increase the maximum snapshot number. This is a status message.

Table 5: PSM Error Codes

Error Code	Description
0xE0001030	Could not dismount volume before starting snapshot restore. The restore operation was canceled. Action: Save the system eventlog and contact technical support.
0xE0001033	An attempt was made to differentiate volumes of unequal length. Action: Save the system eventlog and contact technical support.
0xE0001034	The volume image backup contains one or more corrupt or missing files. Action: Save the system eventlog and contact technical support.
0xE0001036	An exception has occurred. The data contains the exception record. Action: Save the system eventlog and contact technical support.
0xE0001037	Cannot log on to remote server. Action: Save the system eventlog and contact technical support.
0xE0001038	A backup could not be started because a backup was already in progress. Action: None. This is a status message only.
0xE0001039	Canceled by user. Action: None. This is a status message only.
0xE000103A	The restore of the multiple-volume snapshot was disabled. Action: None. This is a status message only.
0xE000103B	The volume does not have enough free cache to perform the restore. Action: Save the system eventlog and contact technical support.
0xE000103C	The restore operation failed. Action: Save the system eventlog and contact technical support.
0xE000103D	Cannot find space to extend cache file because free space detection is disabled. Action: Save the system eventlog and contact technical support.
0xE000103E	Cannot find space to extend cache file because volume contains no snapshots. Action: Save the system eventlog and contact technical support.

index

A

access control list. See ACL
ACL
  defined 92
  translating 121
AFP
  installing services for AppleTalk 100
  installing services for Macintosh 100
  protocol settings 103
  shares, setting up 101
  sharing
  volume mount points 62
alerts, e-mail, setting up 36
AppleTalk. See AFP.
audience 12
Authentication software, installing 109
authorized reseller, HP 16

B

backup
  best practices 155
  hardware options 154
  mappings 126
  multiple devices 155
  readiness testing 158
  schedules 156
  snapshots 42, 157
  software options 154
  solutions 153

C

cache
  changing size 50
  clearing from system 45
  deleting images 50
  full 62
  size 49
  usage 49
caching
  automatic for documents 97
  automatic for programs 97
  manual for documents 97
CIFS
  add a new user or group 97
  modify access 97
  protocol settings 102
  remove access 97
  share support 93
  sharing 96
CIFS administration 64
client groups
  adding NFS 118
  deleting NFS 118
  editing NFS 119
  managing NFS 117
conventions
  document 13
  equipment symbols 13
  text symbols 13

D

data recovery, PSM 41
data replication software
  installing 30
date, system, changing 33
disaster recovery 158
disk quotas
  creating new entries 75
  deleting entries 76
  disabling 74
  enabling 74
  modifying entries 76
document
  conventions 13
  prerequisites 12
  related documentation 13
domain controller
  configuring 64

domain environment 22
drive defragmentation 41
drive quotas
  defined 72
  managing 72

E

e-mail alerts, setting up 36
encoding types 113
environments
  domain compared to workgroup 64
  overview 22
equipment symbols 13
error codes 159
events, SFU, logging 108
explicit mapping 124
explicit mappings 120

F

features
  hard drives 18
  hardward 18
  memory 18
  optional 19
  redundancy 20
  software 19
File and Print Services for NetWare. See FPNW.
file level permissions 86
files, ownership 91
folders
  auditing access 89
  compress tab 83
  creating new 82
  creating new share 84
  deleting 83
  general tab 82
  managing 80
  managing shares for 85
  modifying properties 83
  navigating to 81
FPNW
  accessing 137
  described 135
  installing 136
FTP
  protocol settings 102
  sharing 98

G

getting help 15
granule size
  rules 44
  update utility 44
group names
  examples 65
  managing 65
groups
  adding from a domain 72
  adding local users 71
  adding to permissions list 87
  local, adding 70
  local, deleting 70
  local, managing 69
  local, modifying properties 71
  properties, general tab 71
  properties, members tab 71
  removing local users 72

H

hard drives
  in server 18
hardware, backup 154
help, obtaining 15
HP
  authorized reseller 16
  storage website 16
  technical support 15
HTTP protocol settings 102

I

image directory 48
image groups 54
inactive period 47
inactive time-out 48

L

localhost 107
locks, NFS 115
logging, SFU events 108
logs
  accessing 35
  audit 35
  options 35

M

Macintosh, installing services for 100
managing system storage 28
mapping
  best practices 121
  data stored 122
  explicit 124
  simple 123
mappings
  backup and restore 126
  creating 122
  explicit 120

NFS 120
simple 120
squashed 121
media
offsite storage 156
rotation 156
memory 18
Microsoft Services for UNIX. See SFU
mount points 62

N

NAS B2000
defined 18
desktop 25
hardware features 18
restarting 34
setup information archive 156
shutting down 34
software features 19
utilities 20
NAS Data Copy
described 30
installing 31
NAS Management Console 26
NCP
adding new user 99
creating new share 140, 144
propeties, modifying 142
protocol settings 102
removing access 99
shares, deleting 141
shares, modifying properties 147
sharing 99
NetWare
adding local users 138
enabling user accounts 139
installing services for 136
supervisor account 139
volume mount points 62
Network File System. See NFS.
network interface controllers 18
network settings, changing 37
NFS
async/sync settings 115
client groups 117
adding 118
deleting 118
editing 119
compatibility issues 93
deleting shares 111
file share, creating 110
file sharing tests 128
group mappings 120
locks 115
modifying share properties 111
network protocols 106
protocol properties settings 114
protocol settings 102
sharing 98
user mapping server 107
user mappings 120
NIC teams. See Ethernet NIC teams

O

offsite storage, media 156

P

passwords 130
modifying local user's 68
synchronization
advanced settings 131
best practices 130
customizing 133
implementing 131
installing 132
requirements 131
performance, snapshots 43
permissions
file level 86
list
adding users and groups 87
removing users and groups 87
modifying 87
resetting 89
persistent image. See snapshots.
prerequisites 12
properties
editing PSM schedule 52
editing snapshot 58
protocols
AFP settings 103
CIFS settings 102
FTP settings 102
HTTP settings 102
NCP settings 102
NFS properties settings 114
NFS settings 102
parameter settings 101
planning for compatibility 93
supported 22, 63, 101
PSM
accessing 46
creating new schedule 51
creating snapshots 56
data recovery 41
deleting schedule 53
deleting snapshots 57

editing schedule properties 52
editing snapshot properties 58
error codes 159
global settings 47
image directory 48
image groups 54
inactive period 47
inactive time-out 48
managing snapshots 55
overview 39
restore defaults 48
restore snapshot 60
schedules 50
storage limitations 46
undo snapshot changes 59
volume configuration settings 49
volume display 45
volume settings 48

R

rack stability, warning 15
rapid startup utility
defined 20
redundancy 20
related documentation 13
remote access
methods listed 149
remote shell daemon 152
Telnet Server 151
Terminal Services 150
WebUI 150
remote shell 152
Remote Shell Service 129
restarting the server 34
restore
PSM defaults 48
snapshot 60

S

scheduled shutdown 34
schedules
creating new PSM 51
deleting PSM 53
editing PSM properties 52
PSM 50
security
auditing 89
file level permissions 86
ownership of files 91
services for AppleTalk, installing 100
services for Macintosh, installing 100
setup
completing 28
e-mail alerts 36
SFU
commands 129
event logging 108
SFU, described 106
shares
administrative 93
AFP
CIFS tab 96
creating new 84, 94
creating new NCP 140, 144
deleting 95
deleting NCP 141
FTP 98
managing 92
managing for a volume or folder 85
modifying NCP properties 142, 147
modifying NFS properties 111
modifying properties 96
NCP 99, 140
NFS 98
NFS tests 128
NFS, creating 110
NFS, deleting 111
path 85
setting up AppleTalk 101
standard 93
web (HTTP) 98
shutting down the server 34
simple mapping 123
simple mappings 120
snapshots
always keep 41
attributes 40
automated deletion 41
backup 42
creating 40, 56
deleting 57
drive defragmentation 41
editing properties 58
managing 55
maximum number 47
performance impact 43
read/write 40
reading 40
read-only 40
recovering 43
restoring 60
undo changes 59
software
backup 154
data replication 30
installing Authentication 109
updating 37

squashed mappings 121
squashing 107
subfolder, navigating to 81
symbols in text 13
symbols on equipment 13
synchronization 130
system date, changing 33
system storage
  managing 28
system time, changing 33

T

tape libraries 155
technical support, HP 15
Telnet Server
  auditing log 152
  authentication tab 151
  configuring 151
  enabling 151
  sessions information 152
  settings 152
  using 129
Terminal Services
  defined 36
  described 150
  exiting 36
  opening 36
  using 129
text symbols 13
time, system, changing 33
troubleshooting
  PSM error codes 159
  PSM known issues
    PSM
      known issues 62

U

UNIX
  authenticating user access 107
  converting ACL 121
  group ID 107
  remote shell 152
    See also NFS
  Telnet Server 129
  user ID 107
  volume mount points 62
user access, authenticating 107
user interfaces 23
users
  adding to permission list 87
  local
    adding 67
    deleting 67
    managing 66
    modifying properties 68
  names, managing 65
  NetWare
    adding 138
    enabling 139

V

volume settings, PSM 48
volumes
  available for snapshots 48
  creating new share 84
  creating Novell 135
  managing shares for 85
  mount points 62
  navigating to 81
  NCP 140
  PSM configuration settings 49
  re-extending 45

W

warning
  rack stability 15
  symbols on equipment 13
web sharing 98
websites
  HP storage 16
WebUI
  accessing 23
  defined 20
  launching 150
workgroup environment 22